Fordham Journal of Corporate & Financial Law

Volume 8, *Number* 1 2003 *Article* 9

Information Privacy and Internet Company Insolvencies: When a Business Fails, Does Divesture or Bankruptcy Better Protect the Consumer?

Farah Z. Usmani*

*

INFORMATION PRIVACY AND INTERNET COMPANY INSOLVENCIES: WHEN A BUSINESS FAILS, DOES DIVESTITURE OR BANKRUPTCY BETTER PROTECT THE CONSUMER?

Farah Z. Usmani[*]

INTRODUCTION

Between the Internet bubble burst[1] and the current economic recession,[2] corporate bankruptcy filings are increasing.[3] Sales of

---

[*] To Matt.

1. The Internet bubble burst refers to the meteoric rise and overvaluation of Internet company stocks in 1998 and 1999 and the subsequent devaluation and failure of such companies in 2000 and 2001. *See generally* Andres Rueda, *The Hot IPO Phenomenon and the Great Internet Bust*, 7 FORDHAM J. CORP. & FIN. L. 21 (2001); *see also* Francis G. Conrad, *Dot.coms in Bankruptcy Valuations Under Title 11 or www.Snipehunt in the Dark.noreorg/noassets.com*, 9 AM. BANKR. INST. L. REV. 417, 418–20 (2001). For lists of now defunct Internet companies, see generally http://www.disobey.com/ghostsites/ (last visited Sept. 20, 2002), http://www.upside.com/graveyard/ (last visited Sept. 20, 2002), http://www.hoovers.com/news/detail/0,2417,11_3584,00.html (last visited Sept. 20, 2002).

2. *See* David Leonhardt, *Recovery and the Reluctant Consumer*, N.Y. TIMES, Dec. 10, 2001, at C1 ("A chief cause of the current recession has been the sharp decline in business spending, which has fallen as a result of the overcapacity caused by excessive investments in the booming late 90's.").

3. *See PricewaterhouseCoopers: 2001/2002 Bankruptcy Filings Will Exceed Last Recession; 200 Public Company Filings Forecast for 2002—Second Year of Record Levels*, PR NEWSWIRE, Mar. 11, 2002 (citing PRICEWATERHOUSECOOPERS, PHOENIX FORECAST: BANKRUPTCIES AND RESTRUCTURINGS 2002 (2002)) ("The record number of [public company] bankruptcies in 2001 and forecast for 2002 represent a 127% and 77% increase over [the average from 1986–2000] respectively. Private company bankruptcy filings are also expected to show record increases in 2002."); *see also* Avital Louria Hahn, *New Economy, Bad Math; Street Analysts Take a Deserved Rap for Their E-Commerce Valuations*, INVESTMENT DEALERS DIG., Oct. 23, 2000 ("Many companies in [the e-commerce] sector, if not bankrupt, are off 90% of

substantially all of the assets of companies that have opted to close their doors or exit a particular line of business are also increasing.[4] Of course, the creditors of these companies are desperate to maximize their recoveries.[5] None of this is particularly surprising. However, a new problem has arisen in the cases of e-commerce companies seeking to liquidate their assets—their privacy promises to users could prevent the sale of customer lists compiled by the now floundering Internet companies.

The sale of customer lists is not a new method to increase the capital available to failing companies.[6] However, the nature of the contact between consumer and retailer has changed with the advent of e-commerce.[7] Moreover, the manner in which customer lists were compiled in the past and the way they are compiled by Internet companies today differs greatly.[8] The terms under which such information is collected has also changed.[9] Because of these changes in the interactions between buyers and sellers, all customer lists are not treated equally when a company chooses to

---

their highs . . . . Bankruptcies of dot-coms are now as commonplace as IPOs once were.");
http://www.bankruptcydata.com/default.asp (last visited Sept. 19, 2002) (indicating that public company bankruptcy filings in 2000 were 176, in 2001 were 257, in January 2002 were 17, and in February 2002 were 29).

4. *See* Eleni Chamis, *High (and Low) Lights of 2001: Best New Idea: Bid4Assets*, WASH. BUS. J., Dec. 28, 2001 (stating that as the "tech landscape has become littered with Internet failures and consolidations, Bid4Assets has been there to pick up the pieces" by selling the assets of failed businesses in online auctions), *available at*
http://washington.bizjournals.com/washington/stories/2001/12/31/story3.html (last visited Sept. 18, 2002); *see also* Letter from Marc Rotenberg & Andrew Shen, Electronic Privacy Information Center, to Federal Trade Commission & National Association of Attorneys General (May 25, 2001) ("[M]any companies will be merged, acquired or sold off piece by piece in the course of a bankruptcy."), *available at* http://www.epic.org/privacy/internet/etour.html (last visited Sept. 24, 2002) [hereinafter EPIC letter].

5. *See* Harvey L. Tepner, *Value Added, Value Subtracted: Advising the Debtor*, AM. BANKR. INST. J., Apr. 2001; *see also infra* Part II.A.1.

6. *See infra* Part II.B.2.

7. *See infra* Part II.B.2.

8. *See infra* Part II.B.2.

9. *See infra* Part II.B.2.

sell its assets due to bankruptcy or failure.[10]

This Note further explores this conflict. Part I provides an overview of the goals of bankruptcy law and presents the relevant statutes, in both the brick and mortar and Internet business contexts. The section concludes that the goals of bankruptcy law favor the sale of customer lists.

Part II defines the term customer list, discusses the use and sale of customer lists for both traditional brick and mortar businesses[11] and Internet retailers, explains the current legal protections available to e-commerce customers, and considers policy concerns about data privacy and Internet commerce. Part II concludes that there exists a clear conflict between the treatment of customer lists for brick and mortar businesses and e-commerce businesses.

Part III discusses the conflict between the goals of bankruptcy law and the problems of consumer privacy present in e-commerce, which does not generally exist in brick and mortar businesses. Specifically, the discussion focuses on the seminal *Toysmart* case and its consequences on other Internet businesses and concludes that while the *Toysmart* case has caused many Internet retailers to change their policies, the problem has not been permanently resolved. No one has addressed the differing outcomes possible between brick and mortar and Internet sales.

Part IV provides a discussion of currently proposed and pending legislation in the area of e-commerce privacy. This section concludes that while the bills under consideration may resolve the privacy issues of Internet business customers, they will not resolve the fact that different outcomes occur in the e-commerce and brick and mortar retail businesses.

This Note concludes that the treatment of customer lists in bankruptcies and acquisitions differs greatly. Additionally, the differing outcomes in the sale of customer lists in different types of bankruptcy have not been considered by courts, legislators, or even the Federal Trade Commission ("FTC"). Furthermore, this final section proposes that greater public awareness is needed by

10. *See infra* Parts II.C, III.

11. For the sake of brevity, the term brick and mortar in this Note will include mail-order businesses.

consumers, many of whom do not realize that their information is subject to divesture even when they conduct business with traditional brick and mortar businesses. As a result, any pending legislation should aim for a consistent outcome in bankruptcy proceedings and ideally should protect the privacy rights of all consumers, both Internet and traditional.

I. THE IMPLICATIONS OF BANKRUPTCY

When the Internet bubble burst, many e-commerce businesses went out of business, merged with other companies, or declared bankruptcy.[12] For many of these companies, one of their most valuable assets was their customer list.[13] Other valuable intangible assets included domain names,[14] licensed technology,[15] and human capital.[16] In contrast, physical goods, such as computers, desks, stock, and other office equipment have not been in great demand

---

12. *See* Paul Davidson, *Dying Dot-com's Customers Coveted*, USATODAY.COM, June 19, 2001 ("Many [e-commerce businesses] did not file for bankruptcy protection."), *available at* http://www.usatoday.com/life/cyber/tech/2001-01-30-dying-dot-coms.htm (last visited Jan. 24, 2002); *see also* EPIC Letter, *supra* note 4 ("[A]s the e-commerce industry is undergoing a tumultuous period, it is likely that the public and policymakers will continue to confront scenarios [where the sale of a customer list is part of a merger and not an outright sale].").

13. *See* Arlene Weintraub, *E-Assets for Sale—Dirt Cheap*, BUSINESSWEEK ONLINE, May 14, 2001, *available at* http://www.businessweek.com/magazine/content/01_02/b3732716.htm (last visited Jan. 24, 2002); *see also* Scott E. Blakeley, *E-Bankruptcy Creditors' Committees' Implications of the Toysmart.com Case*, MANAGING CREDIT RECEIVABLES & COLLECTION, May 2001; Walter W. Miller & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 779 (2001); Hal F. Morris & Flora A. Fearon, *Texas Attorney General: Privacy Is Not for Sale*, AM. BANKR. INST. J., Oct. 2000; Davidson, *supra* note 12; *accord* John M. Wingate, *The New Economania: Consumer Privacy, Bankruptcy, and Venture Capital at Odds in the Internet Marketplace*, 9 GEO. MASON L. REV. 895, 908 (2001). For a definition and thorough discussion of customer lists, see *infra* Part II.

14. For a discussion of how to value the assets of a dot.com, see generally Conrad, *supra* note 1.

15. *See* Blakeley, *supra* note 13.

16. *See id.*

or of great value.[17] In fact, tangible assets are becoming more and more difficult to sell.[18]

Because of the diminishing value of tangible goods, companies looking to maximize the return for their creditors or shareholders are desperate to sell whatever they can—including customer lists that are protected by promises of privacy.[19] These privacy promises and the goals of defunct companies to maximize the value of their estates have created a conflict that could result in either smaller estates or the sale and dissemination of customer information obtained under a confidentiality promise.[20] Potentially, consumer privacy may be violated in an effort to increase the value of estates. Nonetheless, these days, "[c]ustomer information will likely be one of the most significant assets of a failed Internet business."[21]

A. Duties of Trustees

When a company declares Chapter 7 bankruptcy and seeks liquidation, the U.S. Trustee must appoint a trustee, or serve as trustee itself.[22] "The trustee shall collect and reduce to money the property of the estate for which such trustee serves, and close such estate as expeditiously as is compatible with the best interests of parties in interest."[23] The basic goal of liquidation is to maximize the value of the estate.[24] A responsible trustee will seek to sell the customer list of a defunct e-commerce business, especially where it has greater value than tangible items that are not realizing their true value at sale.

---

17. *See* Weintraub, *supra* note 13 ("[T]angible goods . . . typically go for little more than 30 cents on the dollar.").

18. *See* Weintraub, *supra* note 13. Even intangible goods are getting harder to sell. *See, e.g.*, *id.* (noting that eToys "hasn't been able to sell the warehouse management system it spent two years and $80 million to develop to ensure that 1 million toys would be under Christmas trees on time").

19. *See* Davidson, *supra* note 12.

20. *See infra* Part III.

21. Richard A. Beckmann, *Privacy Policies and Empty Promises: Closing the "Toysmart Loophole,"* 62 U. PITT. L. REV. 765, 772 (2001); *see also* Blakeley, *supra* note 13.

22. *See* 28 U.S.C. §§ 586(a)(1)–(2) (2000).

23. 11 U.S.C. § 704(1) (2000).

24. *See* Wingate, *supra* note 13, at 912; *see also* Blakeley, *supra* note 13.

Likewise, a creditor may opt to create a creditors' committee to aid the trustee.[25] "Members of a creditors' committee owe a duty of trust, responsibility, and undivided loyalty to unsecured creditors" and "[w]hen a committee fails to exercise its duties carefully or a committee makes false or inaccurate statements intending to injure the debtor, members may be subject to suits from the debtor or creditors."[26] Therefore, the creditors' committees also seek to maximize the value of the estate,[27] both for themselves and for the sake of the unsecured creditors they represent.

B. Bankruptcy Basics

A bankruptcy estate "is comprised of all the following property, wherever located and by whomever held . . . all legal or equitable interests of the debtor in property as of the commencement of the case."[28] Moreover, "an interest of the debtor in property becomes property of the estate . . . notwithstanding any provision in an agreement, transfer instrument, or applicable nonbankruptcy law that restricts or conditions transfer of such interest by the debtor."[29]

While there has been a debate as to whether a customer list is property or a contract between the parties,[30] courts have

---

25. *See* 11 U.S.C. § 705 (2000).

26. *See* Blakeley, *supra* note 13.

27. *See id.*

28. 11 U.S.C. § 541(a)(2) (2000).

29. *Id.* § 541(c)(1)(A); *see also* Miller & O'Rourke, *supra* note 13, at 811.

30. For a discussion of the property versus contract theories underlining customer lists, see generally Miller & O'Rourke, *supra* note 13, at 782–807; *see also infra* Part II.B.2 (discussing how customer lists are often treated as trade secrets, implying that they are property); *infra* note 97 and accompanying text (explaining how the tax implications of the sale of customer lists imply that they are property). The bankruptcy court allows the trustee, with the permission of the court, to complete or reject an executory contract. 11 U.S.C. § 365 (2000). An executory contract is "[a] contract that remains wholly unperformed or for which there remains something still to be done on both sides." BLACK'S LAW DICTIONARY 135 (New Pocket ed. 1996). For a brief discussion of whether customer lists as contracts could be binding under 11 U.S.C. § 365, see *infra* note 102.

traditionally classified customer lists as property.[31] As property, customer lists can be sold.[32] "Customer lists 'were intended by Congress to fall within the scope of [Section] 541.'"[33] Even if the lists are considered to be contracts, and not property, bankruptcy courts could allow for the sale of the lists, despite any privacy promises, because of the primary goal to maximize the estate's value.[34] Of course, while allowing such a sale would increase estate value, it would fail to consider the public's interest in keeping its information private[35] or the importance of holding companies to promises they make,[36] which may induce customers to enter into relationships with those businesses,[37] even if such agreements are not legally binding.

Nonetheless, Congress did not intend for the Bankruptcy Code to supercede the rights of regulatory agencies – such as the Federal Trade Commission – in the exercise of their powers.[38] "Thus, where a governmental unit is suing a debtor to prevent or stop violation of fraud, environmental protection, safety, or similar police or regulatory laws, or attempting to fix damages for violation of such a law,"[39] the unit or agency is not subject to the general bankruptcy stay which prevents the "commencement or continuation . . .of a judicial, administrative, or other action or proceeding against the debtor that was or could have been commenced before" the bankruptcy.[40] As such, filing for

---

31. *See, e.g.*, Phillips v. Diecast Mktg. Innovations, L.L.C., 2000 Bankr. LEXIS 615 (Bankr. E.D. Va. 2000); *cf. In re* Prof'l Sales Corp., 48 B.R. 651, 660 (1985) ("If the disputed interest adds great value to the estate, as it does here [where the interest in the property was conditional], it was intended by Congress to fall within the scope of § 541."); *see also* Beckmann, *supra* note 21, at 776.

32. *See generally infra* Part I.

33. Beckmann, *supra* note 21, at 776 (quoting *In re* Prof'l Sales Corp., 48 B.R. 651, 660 (Bankr. N.D. Ill. 1985)).

34. *See* Miller & O'Rourke, *supra* note 13, at 807–11.

35. *See infra* note 69 and accompanying text.

36. *See Eli Lilly Agrees to Improve On-Line Security*, WHITE HOUSE BULL., Jan. 18, 2002 (quoting Howard Beales, FTC Protector of Consumer Information).

37. *See id.*

38. *See* S. Rep. No. 95-989, at 109-10 (1978), *reprinted in* 1978 U.S.C.C.A.N. 5787, 5838; *see also* Beckmann, *supra* note 21, at 777.

39. *See* Beckmann, *supra* note 21, at 777.

40. *See* 11 U.S.C. § 362(a)(1) (2000); *see also* Beckmann, *supra* note 21, at

bankruptcy is not meant to prevent the FTC from enforcing privacy promises. However, because the bankruptcy court retains jurisdiction over a debtor's assets, such as a customer list, it could "still retain discretion to decide that the bankruptcy process supersedes the consumer protection laws."[41]

Aside from the above, a bankruptcy court:

> may issue any order, process, or judgment that is necessary or appropriate to carry out the provisions of this title. No provision of this title providing for the raising of an issue by a party in interest shall be construed to preclude the court from, sua sponte, taking any action or making any determination necessary or appropriate to enforce or implement court orders or rules, or to prevent an abuse of process. [42]

This allows bankruptcy courts to act "as courts of equity, and [they] are authorized to issue any order, process or judgment that is necessary and appropriate to carry out the provisions of the [Bankruptcy] Code."[43] Clearly, the above discussion demonstrates that the powers of the bankruptcy courts are quite broad.

II. THE USE OF AND LEGAL STATUS OF CUSTOMER LISTS

The scope of customer lists has grown with the development of technology.[44] While some aspects of consumer protection have been addressed in the legal arena, including the sale of customer lists in the brick and mortar context,[45] the sale of similar e-

---

777. *But see In re* Prof'l Sales Corp., 48 B.R. 651, 658, 660–61 (Bankr. E.D. Ill. 1985) (granting an injunction in favor of a bankrupt company and overriding the claims of sovereign immunity by the Environmental Protection Agency ("EPA") and its decision to disallow the bankrupt company's use of its property until the agency could review the debtor's application. The EPA's decision adversely affected the value of the property because "sovereign immunity is largely waived in the bankruptcy context;" "the grant of an injunction would harm the EPA minimally;" "there is a strong policy in favor of successful rehabilitation of debtors;" and the debtor company would suffer harm without the injunction).

41. Beckmann, *supra* note 21, at 778.

42. 11 U.S.C. § 105 (2000).

43. Beckmann, *supra* note 21, at 778–79.

44. *See infra* Part II.C.1.

45. *See infra* Part II.B.2.

commerce lists has not been specifically dealt with.

A. What Is a Customer List?

"A customer list is literally just that—a list of customers."[46] Traditionally, these lists included names,[47] addresses,[48] phone numbers,[49] and perhaps billing information.[50] This information is given by customers in order to pay for and receive the order. According to former FTC official Peter Ward, "[i]n the brick-and-mortar world, you give your name and information as part of a transaction, and there is typically no representation on the part of a seller that that information will be protected."[51]

"The aggregate customer list is more than the simple sum of its parts. The [company's] ingenuity, innovation and effort in compiling the list make it valuable. It is the list that has value, not the information of one particular customer."[52]

In addition to information directly compiled by retailers, companies also have the option of purchasing lists from data brokers.[53] Such information varies from medical information[54] to

---

46. Miller & O'Rourke, *supra* note 13, at 782 (stating that a customer list "may be more or less detailed, containing simply basic information like names and addresses, or exhaustive data on a customer's financial position and shopping preferences.").

47. *See id.* at 783; *see also* Morris & Fearon, *supra* note 13.

48. *See* Miller & O'Rourke, *supra* note 13, at 783; *see also* Morris & Fearon, *supra* note 13.

49. *See* Vince Salas, *CPNI—Coping with Compliance*, WIRELESS REV., Feb. 1, 1999; *see also* Morris & Fearon, *supra* note 13.

50. *See* Don F. Farineau & Royce E. Chaffin, *Amortizing Intangible Assets*, NAT'L PUB. ACCT., Aug. 1992, at 32; *see also* Morris & Fearon, *supra* note 13.

51. Jennifer Jones & James Evans, *Web Privacy Lapse by E-tailer Toysmart Prompts FTC Action*, INFOWORLD, July 17, 2000, at 26.

52. Miller & O'Rourke, *supra* note 13, at 813.

53. Many companies sell customer information, including Acxiom, *available at* http://www.acxiom.com/DisplayMain/0,1494,USA~en~519~2537~0~0~,00.html (last visited Sept. 19, 2002) [hereinafter Acxiom] (selling consumer, business, and telephone data) and MSS Inc., *available at* http://www.mmslists.com/ (last visited Sept. 19, 2002) [hereinafter MSS] (selling healthcare lists, including personal medical information), VentureDirect Worldwide, *available at* http://www.venturedirect.com/scripts/index.php?home (last visited Sept. 19, 2002)

hobbies[55] to ethnicity.[56] Customer lists can also be purchased from competitors or other businesses.[57]

However, due to the advent and rapid development of the Internet,[58] a significant portion of purchasing occurs online.[59] The nature of the Internet and online transactions have increased the amount of information retailers can collect about buyers and visitors.[60]

Additionally, many software companies are now offering

[hereinafter VentureDirect] ("VentureDirect offers online and offline media, to cost-effectively reach virtually every business and consumer marketplace."); *see also* Joel R. Reidenberg, *E-Commerce and Privacy Institute for Intellectual Property & Information Law Symposium: E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 723 (2001) (discussing how Acxiom offered a customer list which identified "individuals who may speak their native language, but do not think in that manner, but withdrew the description from their website after receiving negative publicity.").

54. *See* MSS, *supra* note 53.

55. Polk Automotive Intelligence, *available at* http://www.polk.com/products/markets/dealers_is/target_marketing.asp (last visited Sept. 20, 2002).

56. *See* Acxiom Specialty Lists, *available at* http://www.acxiom.com/DisplayMain/0,1494,USA~en~938~976~0~0,00.html (last visited Sept. 20, 2002) [hereinafter Acxiom Specialty Lists].

57. *See infra* Part II.B.2.

58. *See* Frank Thorsberg, *Growth in Internet Use Slows*, PC WORLD.COM, Aug. 18, 2001 (stating that "the popularity of the Internet continues to grow," but growth will slow down in the future), *available at* http://www.pcworld.com/news/article/0,aid,58043,00.asp (last visited Mar. 20, 2002).

59. *See* Jeremy Lieb, *1999 U.S./Canada Internet Demographic Study*, COMMERCENET, 1999-2000 (indicating that fifty-five million people were making online purchases in 1999), *available at* http://www.commerce.net/research/stats/analysis/99-USCanda-Study.pdf (last visited Mar. 20, 2002).

60. *See Privacy Online: Fair Information Practices in the Electronic Marketplace Before the Senate Committee on Commerce, Science, and Technology*, 106th Cong. (2000) ("[T]echnology has enhanced the capacity of online companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their Web sites."), *available at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (last visited Mar. 20, 2002) [hereinafter Pitofsky testimony] (statement of Robert Pitofsky, Federal Trade Commission); *see also* Wingate, *supra* note 13, at 897.

products to allow Internet businesses to compile more complex customer lists.[61] Now information in the customer lists of Internet companies includes names, addresses, phone numbers, credit card information, shopping history, and web-surfing habits.[62] This information can then be analyzed for patterns and trends, known as data mining, for marketing purposes.[63]

Traditional customer lists were rather simple[64] and were not compiled with any obligation of privacy to those included.[65] Today's lists are far more complex[66] and information compiled from Internet transactions is often obtained with promises of privacy.[67] Due to the fears of misuse of personal information on the Internet,[68] most e-commerce sites have promised to protect the privacy of their customers.[69] Privacy policies are essential to the

---

61. Such software includes SmartBiz, *available at* http://www.fmc-apgspec.com/smartbizp.htm (last visited Mar. 20, 2002); MerchantReach, *available at* http://www-3.ibm.com/software/webservers/commerce/retailindustry.html (last visited Mar. 20, 2002); and Microsoft Great Plains Business Solutions, *available at* http://www.microsoft.com/catalog/display.asp?subid=22&site=10939&x=20&y=14 (last visited Mar. 20, 2002).

62. *See* Davidson, *supra* note 12; *see also* Miller & O'Rourke, *supra* note 13, at 779; *infra* Part III.C.1.

63. *See* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 106–07 (2000). There is currently a debate on whether data mining violates privacy rights, but whether or not it does is outside of the scope of this Note.

64. *See* Miller & O'Rourke, *supra* note 13, at 776–77 (noting that customer lists in the past were "bare-bones" lists).

65. *See supra* note 51 and accompanying text.

66. *See supra* note 51 and accompanying text (noting that new lists gathered using technology are easier to gather and "are simply maintained, manipulated, and transferred").

67. *See supra* notes 68–70 and accompanying text.

68. *See* Wingate, *supra* note 13, at 915 (citing Pitofsky testimony, *supra* note 60); *see also* Beckmann, *supra* note 21, at 771 ("[O]verwhelming majorities of net users say that privacy policies are important, or would matter to them in deciding whether to trade information for benefits, or would increase their Internet usage, purchases, or information disclosure."); Reidenberg, *supra* note 53, at 725 ("[T]he Internet will never realize its full potential as a sales medium unless consumers are assured that their transaction information will remain private."); Beckmann, *supra* note 21, at 770–71.

69. *See* Miller & O'Rourke, *supra* note 13, at 780 ("Many [websites] have posted privacy policies on their Web sites, sometimes promising not to share the

choices made by many Internet users.[70] It is because of these changes in the nature of customer lists that they are not similarly treated.[71] The customer lists of Internet companies are simply far more complicated, both in nature and use, than their traditional counterparts, and these changes are significant because information collected about customers using new methods includes matters which they may consider to be private, such as data about health needs, children, and financial status.[72] "It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns."[73]

B. Customer Lists in Brick & Mortar Businesses

Customer lists have existed for a long time in brick and mortar businesses.[74] "For years, brick-and-mortar companies have sold

---

customer's personal data with any third party."); *see also* Beckmann, *supra* note 21, at 771 ("In response [to consumer concerns about privacy], Internet companies are much more attentive to the consumer demand for privacy than their brick-and-mortar counterparts."); Morris & Fearon, *supra* note 13 ("To acquire this sensitive information, many e-tailers make privacy guarantees promising the customer never to disclose to a third party the information they have collected."). The TRUSTe Privacy Seal Program, an online seal program that signifies that the site conforms to its strict privacy requirements, has over 1500 sites registered. *See* http://www.truste.org/users/users_lookup.html (last visited Mar. 20, 2002). However, "[w]eb seal programs are not a substitute for clear independent legal recourse" and "are also unlikely to cover the vast majority of [w]eb sites." Reidenberg, *supra* note 53, at 727–28.

70. *See* Beckmann, *supra* note 21, at 771.

71. *See infra* Parts II.B–II.C.

72. *See* Lois R. Lupica, *Financing the Enterprises of the Internet: The Technology-Rich "Dot-Com" in Bankruptcy*, 53 ME. L. REV. 361, 376 (2001).

73. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/toc.htm and http://www.ftc.gov/reports/privacy3/conclu.htm (last visited May 2, 2002).

74. *See* Miller & O'Rourke, *supra* note 13, at 778 ("For years, firms have been licensing and selling . . .customer data both in and out of bankruptcy without much fear of legal limitation." Customer lists have been used as collateral for raising capital, have allowed to be licensed, and are subject to sale.); *see also* Wingate, *supra* note 13, at 896.

their customer lists as an asset."[75] There are several reasons why businesses would be interested in purchasing customer lists offered for sale.[76] The sale of such compiled information has been recognized as legitimate in many federal and state courts.[77] These courts have treated customer lists as trade secrets.[78] Other attempts to prohibit the disclosure of customer information by those on lists have also failed.[79] In fact, the sale of customer information in a traditional list has never been prohibited by a bankruptcy court or other court.[80]

1. Incentives to Buy Customer Lists

There are several reasons why one company would want to purchase the customer list of another company. "A dot-com's customer list may be valuable to its competitors because it contains information concerning buying preferences, names and ages of children, credit card numbers, birth dates, and other information that customers may not wish to disclose to third parties."[81] Other reasons to buy customer lists are the potential accuracy of the lists, the fact that they are targeted to specific customers, the opportunity to use such information for product development, and tax incentives.

Accuracy in customer lists is valued because it eliminates waste from incorrect contact information on such lists.[82] Accuracy also revolves around identifying the individual members of a single household, so that each member can be individually targeted.[83] On

---

75. Blakeley, *supra* note 13; *see also* Beckmann, *supra* note 21, at 776 ("In the United States, personal information has long been bought and sold with the assumption that it belongs to the one who compiles it.").

76. *See infra* Part II.B.1.

77. *See infra* Part II.B.2.

78. *See infra* Part II.B.2.

79. *See infra* Part II.B.3.

80. *See infra* Parts II.B.2–II.B.3.

81. Blakeley, *supra* note 13.

82. *See* Sheila Yount, *Quantum Leap: The New Acxiom Data Network Expands Market for Data Services*, ARK. DEMOCRAT-GAZETTE, Mar. 3, 1998, at D1 (noting that accuracy "which will reduce the amount of mail sent to the 'current occupant' or to people who previously lived at an address.").

83. *See* Ralph Kimball, *Dealing with Dirty Data; Data Warehousing;*

the other hand, inaccuracy in customer lists can "cause serious damage to a company, leading to bad decisions, product recalls - even financial losses."[84] Thus it is essential to maintain or obtain an accurate customer list to maximize the effect of marketing and minimize losses. "The bottom line: The right information will pay for itself."[85]

Another advantage of purchasing customer lists is that the lists are targeted, which allows information to be sent to people with a known or demonstrated interest in particular products or services.[86] Additionally, contact made from customer lists could focus on consumers with certain demographic and behavioral characteristics that will make them interested in the products and services offered.[87] When all the members of a household are known, the company can meet "the overall needs of the household and suggest an effective consolidation or expansion of products."[88] Targeted customer lists help to increase effectiveness and reduce losses.

Customer lists compiled by companies based on purchases tend to be more accurate and targeted than lists that can be purchased commercially from companies like Acxiom[89] and VentureDirect.[90] Such lists are comprised of customers who have already demonstrated an interest in a particular product or service and a willingness to purchase online. Because of these attributes of customer lists, it is clear that there is and will continue to be a market for them, either as part of a merger or part of a bankruptcy

---

Technology Info, DBMS, Sept. 1996, at 55.

84. Linda Wilson, *The Devil in Your Data—Hoping to Combine Databases? Be Prepared to Find Inaccurate Information that Can Lead to Unhappy Customers, Useless Reports, and Financial Losses*, INFORMATIONWEEK, Aug. 31, 1992, at 48.

85. John Rendleman, *Customer Data Means Money: Businesses Are Buying and Selling Customer Data in a Dizzying Number of Ways*, INFORMATIONWEEK.COM, Aug. 20, 2001, *available at* http://www.informationweek.com/story/IWK20010816S0008 (last visited Sept. 1, 2002).

86. *See* Yount, *supra* note 82, at D1.

87. *See* Kimball, *supra* note 83.

88. *See id.* (referring to this process as cross-selling).

89. *See* Acxiom, *supra* note 53; *see also* Acxiom Specialty Lists, *supra* note 56.

90. *See* VentureDirect, *supra* note 53.

sale.[91]

Moreover, customer lists can be used for further product development.[92] "Customer knowledge can also help an organization predict which sorts of services and support offerings customers are likely to want or need, and to develop more effective strategies for meeting these needs before they are even articulated."[93] If done properly, such product development could build customer loyalty and develop long term relationships.[94]

Aside from the uses of customer lists, there are tax advantages to purchasing customer lists. "To the extent a transaction can be structured favorably to preserve any carryforwards or minimize any future restrictions, [it] may translate into a [b]uyer's ability to pay more for that business."[95] The fact that a purchased list can be deducted or amortized[96] for fifteen years[97] encourages such sales. The amount deducted or amortized is based on the market value price of the list, not its historical cost, thereby increasing the tax value of the purchase.[98]

2. Customer Lists As Trade Secrets

While the goal of bankruptcy law, to maximize the value of the

---

91. For a discussion on how to value customer lists, see generally Jack Schmid, *Assigning Value to Your Customer List*, CATALOG AGE, Apr. 2001.

92. *See* Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEG. STUD. 561, 574 (1998).

93. Eric Lesser et al., *Managing Customer Knowledge; Becoming 'Customer-Centric' Is Easier Said Than Done. But It Can Be Done.*, J. BUS. STRATEGY, Nov. 2000.

94. *Will You Please Care for My Every Need*, PRECISION MARKETING, June 9, 1997, at 13.

95. *Tax Implications on the Sale of a Business*, *available at* http://www.mediamergers.com/taximplications.html (last visited Sept. 24, 2002) [hereinafter *Tax Implications*].

96. Amortization is defined as "apportioning the initial cost of a usu[ally] intangible asset, such as a patent, over the asset's useful life." BLACK'S LAW DICTIONARY 32 (New Pocket ed. 1996).

97. *Tax Implications*, *supra* note 95. Amortizing or deducting the value of the customer lists implies that the lists are considered property.

98. Thomas Cuccia, *Let's Make a Deal*, SUCCESS, *available at* http://www.fmvopinions.com/deal/htm (last visited Jan. 24, 2002).

debtor estate,[99] and the promises of privacy by Internet businesses[100] are clearly at odds, no one on a customer list has ever challenged its sale in a bankruptcy court.[101] In other proceedings, however, customer lists have been recognized as assets of a company. Many state and federal courts have held that customer lists are trade secrets.[102] Forty-two states and the District of Columbia have adopted the Uniform Trade Secrets Act ("UTSA")[103] drafted by the National Conference of Commissioners on Uniform State

---

99. *See supra* Part I.A.

100. *See supra* notes 51–53 and accompanying text.

101. A recent search on Lexis produced no results.

102. *See* Miller & O'Rourke, *supra* note 13, at 787–88, 806 (stating that as trade secrets, customer lists would be considered property and even if such lists could be treated as contracts between the purchaser and the company compiling the customer information, it is unlikely the trustee would assume the contract and follow through with the agreement per 11 U.S.C. § 365 because (1) there would be no benefit to the estate from assuming the agreement not to disclose the information and (2) the contract between the customer and the seller need not be considered executory, as the customer had already provided his or her information and the seller had already provided the service or product); *see also supra* note 30.

103. *See* ALASKA STAT. § 45.50.910 (2001); ARIZ. REV. STAT. § 44-401 (Michie 2001); ARK. CODE ANN. § 4-75-601 (Michie 2001); CAL. CIV. CODE § 3426 (Deering 2001); COLO. REV .STAT. § 7-74-101 (2001); CONN. GEN. STAT. § 35-50 (2001); DEL. CODE ANN. tit. 6 § 2001 (2001); D.C. CODE ANN. § 48-501 (2001); FLA. STAT. ch. 688.001 (2001); GA. CODE ANN. § 10-1-760 (2001); HAW. REV .STAT. § 482B-1 (2001); IDAHO CODE § 48-801 (Michie 2001); 765 ILL. COMP. STAT. § 1065/1 (2001); IND. CODE § 24-2-3-1 (2001); IOWA CODE § 550.1 (2001); KAN. STAT. ANN. § 60-3320 (2001); KY. REV.STAT. ANN. § 365.880 (2001); LA. REV. STAT. ANN. § 51:1431 (West 2001); ME. REV. STAT. ANN. tit. 10 § 1541 (West 2001); MD. CODE ANN. [COM. LAW] § 11-1201 (2000); MICH. COMP. LAWS § 445.1901 (2001); MINN. STAT. § 325C.01 (2001); MISS. CODE ANN. § 75-26-1 (2001); MO. REV. STAT. § 417.450 (2001); MONT. CODE ANN.§ 30-14-401 (2001); NEB. REV. STAT. § 87-501 (2001); NEV. REV. STAT. § 600A.010 (2001); N.H. REV. STAT. ANN. § 350-B:1 (2001); N.M. STAT. ANN. § 57-3A-1 (2001); N.C. GEN. STAT. § 66-152 (2001); N.D. CENT. CODE § 47-25.1-01 (2001); OHIO REV. CODE ANN. § 1333.61 (Anderson 2001); OKLA. STAT. tit. 78 § 85 (2001); OR. REV. STAT. § 646.461 (2001); R.I. GEN. LAWS § 6-41-1 (2001); S.C. CODE ANN. § 39-8-1 (Law. Co-op 2001); S.D. CODIFIED LAWS § 37-29-1 (Michie 2001); UTAH CODE ANN. § 13-24-1 (2001); VT. STAT. ANN. tit. 9, § 4601 (2001); VA. CODE ANN. § 59.1-336 (Michie 2001); WASH. REV. CODE § 19.108.010 (2001); W. VA. CODE § 47-22-1 (2001); WIS. STAT. § 134.90 (2001).

Law.[104] Section 1(4) of the UTSA defines trade secret as:

> 4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[105]

"Many customers lists compiled by e-tailers are likely to fit this definition. They derive at least part of their value from not being known to competitors and are usually the subject of reasonable efforts to maintain their secrecy."[106]

California[107] has adopted the UTSA[108] and has recognized that customer lists can be sold.[109] Courts have held that, "customer lists and related information may constitute protectable [sic] trade secrets."[110] Other UTSA states have reached similar conclusions.[111]

---

104. *See* http://www.execpc.com/~mhallign/usta.html (last visited Mar. 20, 2002).

105. UNIF. TRADE SECRETS ACT § 1(4) (amended 1985).

106. Miller & O'Rourke, *supra* note 13, at 788.

107. For the sake of brevity, California is used as an example of a state that has adopted the UTSA.

108. *See* CAL. CIV. CODE § 3425 (Deering 2001); *see also* Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1520-21 (Cal. App. 1st Dep't Super. Ct. 1997); Courtesy Temp. Serv., Inc. v. Camacho, 222 Cal. App. 3d 1278, 1286-87 (Cal. App. 2nd Dep't Super. Ct. 1990); Am. Paper & Packaging Prods., Inc. v. Kirgan, 183 Cal. App. 3d 1318, 1322-23 (Cal. App. 2nd Dep't Super. Ct. 1986); Linda L. Castle, *Computers and High Tech, Revisited*, 1 A.B.A.J. 150 (1985).

109. *See, e.g.*, Stewart v. Telex Communications, Inc., 1 Cal. App. 4th 190, 193 (Cal. App. 3rd Dep't Super. Ct. 1991); Lundell v. Sidney Mach. Tool Co., 190 Cal. App. 3d 1546, 1553 (Cal. App. 2nd Dep't Super. Ct. 1987); Harvey v. White, 213 Cal. App. 2d 275, 276 (Cal. App. 3rd Super. Ct. 1963).

110. Gemini Aluminum Corp. v. Cal. Custom Shapes, Inc., 95 Cal. App. 4th 1249, 1263 (Cal. App. 4th Dep't Super. Ct. 2002).

111. *See* Richard A. Bales & Joseph S. Burns, *A Survey of Kentucky Employment Law*, 28 N. KY. L. REV. 219, 269 (2001) ("[O]ther states have defined trade secrets to include customer lists."); *see also* Denise H. McClelland & John L. Forgy, *Is Kentucky Law "Pro-Business" in Its Protection of Trade Secrets, Confidential and Proprietary Information? A Practical Guide for*

Seven states have recognized trade secrets under common law.[112] For example:

> In determining whether information constitutes a trade secret, New York[113] courts have considered the following factors: (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[114]

Moreover, any customer list compiled through the efforts of the business and which remains confidential is a trade secret.[115] As a result, several courts have recognized the legitimacy of the sale of customer lists.[116]

Two states have drafted their own privacy provisions relating

---

Kentucky Businesses and Their Lawyers, 24 N. KY. L. REV. 229, 231 (1997).

112. These states are Missouri, New Jersey, New York, Pennsylvania, Tennessee, Texas, and Wyoming. *See* http://execpc.com/~mhallign/42state.html (last visited Mar. 20, 2002). For a discussion of how trade secrets at common law were enforced under both contact and property theories, see Milton E. Babirak, Jr., *The Virginia Uniform Trade Secrets Act: A Critical Summary of the Act and Case Law*, 5 VA. J.L. & TECH. 15 (2000).

113. For the sake of brevity, New York will be used as an example of states recognizing customer lists as trade secrets under common law for the sake of brevity.

114. *See* N. Atl. Instruments v. Haher, 188 F.3d 38, 44 (2d Cir. 1999) (citing Restatement of Torts § 757 cmt. B); *see also* Simplex Wire & Cable Co. v. Dulon, Inc., 196 F. Supp. 437, 441 (E.D.N.Y. 1961); Ferranti Elec., Inc. v. Harwood, 251 N.Y.S.2d 612, 618 (N.Y. Sup. Ct. 1964).

115. *See N. Atl. Instrument*, 188 F.3d at 38.

116. *See, e.g.*, Roessel Cine Photo v. Kapsalis, No. 109251/96, 1997 N.Y. Misc. LEXIS 299 (N.Y. Sup. Ct. 1997); Danna Metro Heating Corp. v. Mobil Oil Corp., 203 A.D.2d 231 (N.Y. Sup. Ct. 1994); Murphy Heating Serv., Inc. v. Chu, 124 A.D.2d 907 (N.Y. Sup. Ct. 1986). As noted in the discussion about USTA states, no customer on a list has ever challenged the sale of a customer list in the bankruptcy context, so these cases have not considered privacy issues. *See supra* note 109.

to the nature of customer lists as trade secrets.[117] In Alabama, lists have been protected as trade secrets where they "have contained specific information about customers" and "in those cases, the information was treated by the claimant as secret."[118] Many Alabama courts have recognized the legitimacy of selling customer lists.[119]

Likewise, in Massachusetts, "if the person entitled to a trade secret wishes to have its exclusive use in his own business, he must not fail to take all proper and reasonable steps to keep it a secret."[120] As such, the legitimacy of the sale of customer lists is also recognized in that state.[121]

As the above demonstrates, all states recognize customer lists as trade secrets under certain circumstances. Similarly, trade secrets are protected under federal law. Pursuant to 18 U.S.C. § 1839(3):

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how

---

117. *See* ALA. CODE § 8-27-1 (2001) (effective Aug. 12, 1987); *see also* MASS. GEN. LAWS. ch. 93, § 42 (2001) (effective 1967).

118. Public Sys., Inc. v. Towry, 587 So. 2d 969, 973 (Ala. 1991); *see also* Birmingham Television Co. v. DeRamus, 502 So. 2d 761 (Ala. Civ. App. 1986).

119. *See, e.g.*, Brown v. Economy Baler Co., 599 So. 2d 1 (Ala. 1992); Specialty Container Mfg., Inc. v. Rusker Packaging Inc., 572 So. 2d 403 (Ala. 1990); James v. Mc Coy Mfg., Co., 431 So. 2d 1147 (Ala. 1983). As mentioned in the USTA and common law state discussions above, no one in Alabama has ever challenged the sale of a customer list in the context of bankruptcy. *See supra* notes 109, 116.

120. J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 357 Mass. 728, 738 (1970); *see also* Export Lobster Co. v. Bay State Lobster Co., No. 92-6348-E, 1994 Mass. Super. LEXIS 90, at *19 (Sup. Ct. 1994); *In re* Yankee Milk, Inc., 372 Mass. 353, 363 (1977).

121. *See, e.g.*, Christian Book Distribs., Inc. v. Wallace, 533 Mass. App. Ct. 905 (App. Ct. 2002); Coastal Oil New England v. Citizens Fuels Corp., 388 Mass. App. Ct. 26 (App. Ct. 1995); Frontier Enterprises, Inc. v. Anchor Co. of Marblehead, Inc., 404 Mass. 506 (1989). Again, no one in Massachusetts has ever challenged the sale of a customer list because his name was included. *See supra* notes 109, 116, 119.

> stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.[122]

Although no federal court has applied § 1839 to hold customer lists to be trade secrets, probably because most such disagreements fall under state contract law,[123] the statute could certainly be read to allow such an interpretation. Nonetheless, federal courts, namely bankruptcy courts, have recognized the legitimacy of selling customer lists.[124]

Clearly, there are many reasons for a party to purchase a customer list from another business and such sales have been allowed nationwide, both under state law and federal law, especially in bankruptcy cases, for traditional brick and mortar businesses. However, as will be shown below,[125] such sales are sometimes problematic for Internet businesses.

3. Other Causes of Action When Consumer Information Is Disclosed

Individuals have tried various causes of action to prevent the dissemination of information on customer lists. In *Dwyer v. American Express Co.*, a class action suit was filed against a credit card company for renting information about customer shopping

---

122. 18 U.S.C. § 1839(c) (2000).

123. Federal courts have abided by state court findings that customer lists are trade secrets. *See, e.g.*, U.S. v. Martin, 228 F.3d 1 (1st Cir. 2000); N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38 (2d Cir. 1999).

124. *See, e.g.*, *In re* United States Truck Co. Holdings, No. 99-59972-WS, 2000 Bankr. LEXIS 1376 (Bankr. E.D. Mich. 2000); Phillips v. Diecast Marketing Innovations, No. 99-60268-T, 2000 Bankr. LEXIS 612 (Bankr. E.D. Va. 2000); *In re* R & A Assoc., Inc., No. 98-365566F, 1999 Bankr. LEXIS 543 (Bankr. E.D. Penn. 1999). These cases do not include bankruptcy cases because no case challenging the sale of a customer list has never been decided because of dismissal or settlement. *See supra* notes 109, 116, 119, 121; *see also infra* Part III.

125. *See infra* Part II.C.

preferences and habits.[126] The plaintiffs brought both privacy and Illinois consumer fraud claims.[127] The court found that the privacy claims could not be upheld because the plaintiffs could not demonstrate intrusion or prying into their seclusion.[128] Rather, "[b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences . . . a defendant has [not] committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."[129] Similarly, the fraud claim was denied because of a lack of damages, other than an excess of mail.[130] As a result, the dismissal of the case was affirmed.[131]

In a similar case in New York, a group of plaintiffs brought suit against their credit card and mortgage holding company for selling their information to third party vendors without their consent or the chance to remove their names from the lists.[132] The plaintiffs claimed that the defendant engaged in deceptive business practices, received unjust enrichment, breached its contract with the plaintiffs, and violated New York civil rights laws.[133]

In the above case, the New York Court of Appeals affirmed the lower court's dismissal of all of the charges.[134] It found that the deceptive practices claim could not stand because the plaintiffs did not actually suffer any injury.[135] The "class members were merely offered products and services which they were free to decline. This

126. Dwyer v. American Express Co., 273 Ill. App. 3d 742, 743-45 (1995) (noting that the lists were marketed based on types of specific products bought, like fine jewelry, mail-order, or electronics, or based on the likelihood of a customer shopping with a particular retailer, based on shopping habits and recent purchases).

127. *Id.* at 744.

128. *Id.* at 746.

129. *Id.*

130. *Id.* at 750.

131. *Id.* at 751.

132. Smith v. Chase Manhattan Bank, USA, N.A., No. 2000-08199, 2002 N.Y. App. Div. LEXIS 3790, *2–*3 (2001).

133. *Id.* at *2 (noting that no privacy claim was made by the plaintiffs).

134. *Id.* at *3.

135. *Id.* at *4–*6.

does not qualify as actual harm."[136] The claim of unjust enrichment was also dismissed because such a claim requires that the plaintiff not receive adequate compensation for a benefit conferred upon the defendant.[137] "The plaintiffs failed to state a cause of action to recover damages for unjust enrichment since the members of the plaintiffs' class who made purchases of products and/or services received a benefit" – the product purchased.[138] Likewise, the breach of contract claim failed because the damages claimed were vague and redress for emotional distress is not available through a breach of contract allegation.[139] Finally, the civil rights claims were disallowed because those statutes were not intended to resolve issues such as the ones in this case.[140]

C. Customer Lists in E-Commerce

1. How Information Is Collected on the Internet

"[T]he technological developments that have made e-commerce possible also have enhanced the ability of companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their sites on the World Wide Web."[141] Unlike the traditional collection of transactional information in the brick and mortar realm,[142] data on the Internet is essentially collected in two different ways: (1) by compiling information provided by the user during a transaction or survey; and (2) by accessing information about a user without her knowledge or consent.[143]

---

136. *Id.* at *5.
137. *Id.* at *6.
138. *Id.*
139. *Id.* at *7.
140. *Id.* at *7–*8 (providing no further explanation, the court merely stated "[t]he plaintiffs have failed to state a cause of action under Civil Rights Law §§ 50 and 51. Civil Rights Law §§ 50 and 51, which must be narrowly construed, were never intended to address the wrongs complained of by the plaintiffs.").
141. Wingate, *supra* note 13, at 897 (quoting the Federal Trade Commission).
142. *See supra* note 51 and accompanying text.
143. *See* Miller & O'Rourke, *supra* note 13, at 784.

a. User-Provided Information

User-provided information is exactly what it sounds like: data compiled based on information customers give to the party running the Internet site.[144] For example, when placing an order on Amazon.com, the company requires the name of the purchaser, her billing address, a separate shipping address (if applicable), her phone number, her credit card number and its expiration date, and her email address.[145] Likewise, to set up an email account on Yahoo!, the user is asked to provide her name, date of birth, current email address (optional), zip code, gender, profession, job title, professional area of specialty, and can fill out an optional survey on his or her interests.[146]

Additionally, an Internet user may be asked to provide additional information in a survey,[147] brought up as a separate window, after a transaction has been completed, or as an attempt to provide further services to a user, such as recommending other purchases.

b. Accessing User Information

Other information about Internet users is collected through clickstream data, cookies, and web bugs. Clickstream data, essentially determining what sites the user came from, is collected by the website visited, recording "the Internet service provider, the type of computer and software used, the website linked from, the amount of time spent perusing each page, and exactly what parts of the website were explored and for how long."[148] The visited

144. *See id.* at 784.

145. *See generally* http://www.amazon.com/exec/obidos/account-access-login/ref=hy_f_2/002-6570095-1914453 (last visited Mar. 20, 2002).

146. *See* http://edit.yahoo.com/config/eval_register?.intl=&new=1&.done=&.src=ym&partner=&promo=&.last= (last visited Mar. 20, 2002).

147. *See id.*

148. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1411 (2001); *see also* Suzanne M. Thompson, *The Digital Explosion Comes with a Cost*, 4 J. TECH. L. & POL'Y 3, 8 n.7 (1999) (finding that clickstream data is compiled by "a series of electronic markers (trail) at each website or page generated by a user's browsing activities,

website then "collects information about the way [the] user interacts with the site and stores the information in its database" and uses this information to target advertisements and products to the user.[149]

More and more companies are accessing clickstream data for direct marketing and targeted advertising purposes.[150] Such information can be obtained, stored, and used and reused at the leisure of the collecting entity.[151] Moreover, "[t]his aggregation of data is particularly telling if done by a site host of an Internet search engine (e.g., Yahoo!). The search engine site can monitor both the type of information that a user is seeking (patterns of research) and the web sites visited to obtain that information."[152]

Similarly, cookies are small code files placed on computers when a user first visits a particular website and which update information about the user each time the user returns to that website.[153] Once a cookie is placed on a computer, it facilitates the transmission of the users clickstream data to the website operator.[154] One of the purposes of a cookie is to identify which ads a customer sees, which of those ads the customer actually responds to by clicking on it, and which items the customer actually places in her virtual shopping cart.[155]

---

including every page of access, newsgroups participated in, distribution lists received, e-mail addresses sent and received.").

149. Solove, *supra* note 148, at 1411.

150. *See* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 65 (1999/2000). For an argument that clickstream data should be subject to privacy provisions, see *id.*

151. *See* Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95, 100 (1998).

152. *Id.*

153. Wingate, *supra* note 13, at 898. Actually, since the website can only identify the computer and not the actual user, the information collected is specific to the computer which the file is placed on, and not the actual user. Nonetheless, given that many computers are primarily used by one individual (such as an office computer) or by a single household, the information is still meaningful to those collecting it.

154. *See* Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 KAN. L. REV. 641, 645–46 (2001).

155. *See* Wingate, *supra* note 13, at 898 (identifying this purpose as state

Cookies also ascertain whether a user has recently visited the site.[156] This data helps determine how much an advertiser should compensate the website operator for exposing individual visitors to its ads so that the advertiser compensates for exposing a single user to an ad. This prevents an advertiser from compensating per visitor, as the same visitor may return to the cite several times.[157]

However, one of the most significant purposes of cookies is to collect information about users for marketing.[158] This practice, known as online profiling, uses clickstream data to collect and convey information about user preferences based on the websites the user visits.[159] While this information may not be able to directly identify the user, it can ultimately be linked up with identifiable data, thereby revealing the interests and needs of specific people.[160] "By linking the online profiles to personally identifying information, the databases can then be used to narrowly tailor advertisements to individual consumers based on what had previously been anonymous web-surfing."[161]

Companies such as Doubleclick[162] create a network of websites that track user information between sites, so that the company can "compile a database of detailed information about the users, their [I]nternet surfing habits and perhaps even personalized information the users have provided to websites."[163]

In addition to cookies, Internet sites also use web bugs to gather information. "A Web bug is a graphic on a [W]eb page or in an [e]mail message that is designed to monitor who is reading the Web page or Email message . . . [they] are often invisible because they are typically only 1-by-1 pixel in size."[164] Web bugs

---

management).

156. *See* Wingate, *supra* note 13, at 899.

157. *See id.* at 898.

158. *See id.*

159. *See id.*

160. *See id.* at 899–900.

161. *See id.* at 900.

162. *See generally*, http://www.doubleclick.com/us/ (last visited Mar. 22, 2002).

163. Wingate, *supra* note 13, at 899 (quoting Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, PRACTICING LAW INST., June 2000, at 141, 144).

164. *See* Richard M. Smith, *FAQ: Web Bugs, Privacy Foundation, available at*

transmit information such as the IP address of the user's computer, the URL of the page the web bug is place on, the URL of the actual bug, the time the bug was viewed, the type of browser the visitor is using, and any relevant cookie data on the user's computer.[165] Web bugs serve several purposes: (1) to build a profile about the user based on sites she has visited; (2) to determine how many users have visited a certain website; (3) to determine which web browsers are used more often at specific sites; (4) in the case of email, to determine how often messages are actually read and forwarded, as opposed to deleted or ignored; and (5) when placed in an email, to ease identification of the email recipient when she visits the sender's website.[166]

Clearly, clickstream data, cookies, and web bugs all generate and obtain great amounts of information, which can easily be matched up with real people to determine whether John Jones has visited the Viagra website or whether Mary Smith has looked up potty training and purchased toys for a one year old female child.[167] Anonymity can be easily compromised, given the amount of information collected and the number of parties collecting such information.[168] What is worse is that most users are unaware that this additional information is being collected.[169] Almost thirty percent of Internet users are not aware of the existence of cookies, and forty percent of people online do not know how to deactivate them.[170]

As the above illustrates, customer lists in the e-commerce context contain far more information than traditional customer

---

http://www.privacyfoundation.org/resources/webbug.asp (last visited Mar. 22, 2002).

165. *See id.*; *see also* Jenab, *supra* note 154, at 645 n.20.

166. *See* Smith, *supra* note 164.

167. *See* ONLINE PROFILING: A REPORT TO CONGRESS—PART 2 RECOMMENDATIONS, FEDERAL TRADE COMMISSION, July 2000, at 3 ("[I]n some cases, the profiles derived from tracking customers' activities on the Web are linked or merged with personally identifiable information."), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf (last visited Mar. 22, 2002).

168. *See* Wingate, *supra* note 13, at 800.

169. *See* Jenab, *supra* note 154, at 647.

170. *See* Reidenberg, *E-Commerce*, *supra* note 53, at 730 (citing the results of an online Wall Street Journal and Harris Interactive study).

lists compiled by brick-and-mortar businesses.[171] Moreover, much of the information is collected without the knowledge of customers,[172] who may simply believe that the information collected about them is solely the information they provided.

2. Laws Protecting E-Commerce Consumers

There have been several statutes passed to protect Internet users;[173] however, none of these have directly addressed the collection of data without customer knowledge or the transfer of such information. What follows is a brief explanation of the Internet user protection statutes that have been passed, followed by a discussion of how these laws do not adequately address the issue of data collection or sale of such information.

a. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is aimed at anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication."[174] "It is reasonable to interpret this statute as prohibiting the covert, unauthorized collection of personal information of web-users while they are engaged in the acts of interstate or foreign commerce or communication."[175] However, CFAA has a $5,000 minimum damage requirement, during any single year, in civil actions.[176] Because most personal information cannot meet the threshold damages requirement,[177] collection of personal data is not generally

171. *See supra* Part II.A.
172. *See* Jenab, *supra* note 154, at 647.
173. *See* Wingate, *supra* note 13, at 900.
174. *See* 18 U.S.C. § 1030(a)(2)(C) (2000).
175. Wingate, *supra* note 13, at 901.
176. *See* 18 U.S.C. § 1030(e)(8) (2000).
177. *See* Miller & O'Rourke, *supra* note 13, at 786 ("Neither state nor federal law accords a person an exclusive right in his or her name, address or phone number."). For a discussion on the difficulty of valuing such personal information, see *id.* at 802 and n.123.

prosecuted under CFAA. Nonetheless, theoretically, CFAA could be used to prosecute the collection of information using clickstream data, cookies, and web bugs,[178] but to date, it has not been successfully used in such a manner.

A CFAA claim of this nature was brought against Doubleclick in January 2000.[179] Identical claims were consolidated for the purposes of class action in May, 2000, with two other actions combined by September.[180] The *Doubleclick* Court found "that damages and losses under § 1030(e)(8)(A) may only be aggregated across victims and over time for a single act," based on the use of singular, instead of plural, terms in the statute and based on legislative intent.[181] Therefore, because the plaintiffs could easily modify their browser settings to prevent Doubleclick from planting cookies on their computers and because no actual economic damage to computers or data was pleaded by the plaintiffs, the claim was dismissed.[182]

The *Doubleclick* holding was used in *Avenue A*, where the court dismissed the CFAA action because "it is undisputed that each time a web page sends a message to a user's computer instructing the computer to communicate the contents of the cookie on the user's hard drive with Avenue A, it is an individual, singular act."[183] The *Avenue A* Court found that each individual access to a cookie did not result in $5,000 of damage and, therefore, dismissed the action.[184] Other courts have found the threshold damage amount is not met in CFAA cases alleging

178. *See* Fernando Piera, *International Electronic Commerce Legal Framework at the Beginning of the XXI Century*, 10 CURRENTS: INT'L TRADE L.J. 8, 13–14 (2001); *see also News*, NAT'L L.J., Dec. 24, 2001, at A19 ("Until last year [2000], all reported CFFA civil cases involved lawsuits brought for damage to computer-stored data that affected either unsuspecting consumers who allegedly were deliberately provided with defective computer goods . . .or Internet companies whose facilities were used to send unsolicited junk e-mail, known as spam.").

179. *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

180. *Id.*

181. *Id.* at 523.

182. *Id.* at 524-26.

183. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001).

184. *Id.* at 1160.

improper use of cookies.[185]

A CFAA claim was also brought in a civil class action against Toys R Us.[186] There, the CFAA claim survived a summary judgment motion, where the court found that the act of placing identical cookies on the machines of all class action plaintiffs constituted a single act[187] and that the aggregation of damages met the $5,000 threshold.[188] However, the final decision in the case is still pending.

b. The Electronic Communications Privacy Act

Another statute that could prevent the collection of data without user knowledge is the Electronic Communications Privacy Act ("ECPA"), which states that "any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" is subject to civil or criminal liability.[189] The "ECPA could serve as an existing statutory prohibition on the covert collection of personal consumer information" by alleging that cookies are bugs, such as phone taps, and are considered spying.[190] However, ECPA included exceptions where one of the

185. *See, e.g., In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1374–75 (S.D. Fla. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001) (noting that loss means irreparable damage). However, the *Intuit* court did find that the intentional placement of a cookie on a user's computer satisfied the scienter requirement of 18 U.S.C. § 1030. *In re Intuit*, 138 F. Supp. 2d at 1280.

186. *See In re* Toys R Us, Inc. Privacy Litig., No. M-00-1381, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. 2001).

187. Using *Doubleclick* as precedent, the *Toys R Us* Court held that § 1030(e)(8)(A) requires "loss aggregating at least $ 5,000 in value during any 1-year period to one or more individuals," to be caused from a single act. *In re* Toys R Us, Inc. Privacy Litig., No. M-00-1381, 2001 U.S. Dist. LEXIS 16949, at *34 (N.D. Cal. 2001).

188. *See In re Toys R Us, Inc. Privacy Litig.*, 2001 U.S. Dist. LEXIS 16949, at *28–*39.

189. *See* 18 U.S.C. § 2511(a) (2000).

190. *See* Wingate, *supra* note 13, at 902; *see also* Adam R. Fox, *E-Commerce in the Digital Millenium: The LegalNotion of a Constitutional Moment*, 27 RUTGERS COMPUTER & TECH. L.J. 267, 290 n.97 (2001).

parties to a communication intercepts the message or data or if prior consent is given for such interception.[191] "Presumably the statute's exceptions permitting interception and disclosure by 'parties to the communication' exempt the collection, analysis, and disclosure of clickstream data by websites."[192] No action has yet been brought under § 2511(a) of ECPA.

In *Doubleclick*, there was an ECPA Title II claim,[193] under the Stored Electronic Communications Act, which is aimed at anyone who (1) "intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in *electronic storage* in such system shall be punished . . . ."[194] The plaintiffs claimed that the placement of cookies constituted "access without authorization," but like § 2511, there is an exception "with respect to conduct authorized . . . by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user."[195] Doubleclick argued that its affiliates are Internet users and that all accessed communications were intended for these sites.[196] The court held that "the cookie identification numbers sent to DoubleClick from plaintiffs' computers fall outside of Title II's protection because they are not in 'electronic storage' and, even if they were, DoubleClick is authorized to access its own communications.[197] The *Avenue A* and *Toys R Us* courts relied on

191. *See* 18 U.S.C. § 2511(2)(d).

192. Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 75 (1999).

193. *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001).

194. 18 U.S.C. § 2701(a) (2000) (emphasis added).

195. *Doubleclick*, 154 F. Supp. 2d at 507 (quoting 18 U.S.C. § 2701(c)(2)).

196. *Id.*

197. *Id.* at 513–14. The remaining claims were settled on April 29, 2002. Press Release, Doubleclick, Inc., Doubleclick and Plaintiffs Agree to Settle Class Action Privacy Litigation (Mar. 29, 2002), *available at* http://www.doubleclick.com/us/corporate/presskit/press-releases.asp?asp_object_1=&press%5Frelease%5Fid=2584 (last visited May 1, 2002). Doubleclick agreed to post a clear privacy policy, to use information collected in a manner consistent with that policy, give consumers the opportunity

this holding for dismissing the Title II ECPA claims in those cases.[198]

c. The Federal Trade Commission Act

What has been most successful in the protection of consumer data has been the Federal Trade Commission Act ("FTCA"), a statute passed well before the advent of Internet technology.[199] Pursuant to the FTCA, the FTC is empowered to prevent "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[200] This broadly worded statute allows the FTC to bring actions against the sale of customer lists compiled while under a privacy commitment.[201]

An action under the 15 U.S.C. § 45 can be based on any misrepresentation that induces a customer to opt to deal with a

---

to opt-in before information collected would be matched to personally identifiable information, undertake a consumer education effort, to regularly purge consumer information that is collected, and limit the life of cookies placed on computers to five years. *Id.*

198. *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. Sept. 14, 2001) ("[W]eb sites are users of the electronic communication service provided, as Plaintiffs allege, by personal computers accessing the Internet, and Avenue A's alleged access of the communications between personal computers and web sites is authorized by the web sites."); *see also In re* Toys R Us, Inc. Privacy Litig., No. M-00-1381, 2001 U.S. Dist. LEXIS 16949, *6-*14 (N.D. Cal. Oct. 9, 2001).

199. *See* Barbara Crutchfield George, et al., *U.S. Multinational Employers: Navigating Through the 'Safe Harbor" Principles to Comply With the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 777 (2001) (noting that the FTCA was enacted in 1914).

200. 15 U.S.C. § 45(a) (2000).

> [I]f it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint.

Id. § 45(b).

201. *See infra* Part III.A; *see also* FTC v. Colgate-Palmolive Co., 380 U.S. 374, 384 (1965) ("[T]he Commission is often in a better position than are courts to determine when a practice is 'deceptive' within the meaning of the [FTC] Act.").

specific company.[202] The deception need not result in any injury: "[d]eception itself is the evil the statute is designed to prevent."[203] "A good society depends upon promises being kept. And individuals in society have a right to be told the truth so that their choices among products, or, as in this case, among offers, can be understandingly made."[204] "All that is required is a showing that the acts and practices were capable of being interpreted in a misleading way. Testimony of consumers that they were mislead is sufficient to sustain a prima facie case of unfair and deceptive trade practices."[205]

The FTC first brought its first privacy action against GeoCities.[206] In its complaint, the FTC alleged that "[GeoCities] has also sold, rented, or otherwise marketed or disclosed this information, including information collected from children, to third parties who have used this information for purposes other than those for which members have given permission."[207] Hence, the dissemination of information rendered the privacy provisions false or misleading.[208]

GeoCities opted to settle the case and agreed to update and clarify its privacy policy to accurately indicate how the collected information would actually be used.[209]

> The order would require the company to post on its site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove

---

202. *See Colgate-Palmolive*, 380 U.S. at 386.

203. *See* Floersheim v. FTC, 411 F.2d 874, 878 (9th Cir. 1969) (citing *Colgate-Palmolive*).

204. Spiegel Inc. v. FTC, 494 F.2d 59, 63 (7th Cir. 1974).

205. Beckmann, *supra* note 21, at 775.

206. *See* Press Release, Federal Trade Commission, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), *available at* http://www.ftc.gov/opa/1998/9808/geocitie.htm (last visited May 1, 2002); *see also* Complaint, *In re* Geocities (FTC 1998) (No. 982-3015), *available at* http://www.ftc.gov/os/1998/9808/geo-cmpl.htm (last visited Mar. 25, 2002).

207. *See* Complaint, *supra* note 206, ¶ 14.

208. *See id.* ¶ 16; *see also* Wingate, *supra* note 13, at 908.

209. *See* FTC Release, *supra* note 206; *see also* Wingate, *supra* note 13, at 909.

> the information. The Notice, or a clear and prominent hyperlink to the Notice, would have to appear on the Web site's home page and at each location on the site at which such information is collected.
>
> The order also would prohibit GeoCities from misrepresenting either the identity of a party collecting any personal identifying information or the sponsorship of any activity on its Web site.[210]

Because of the settlement of *GeoCities* and other similar cases, no court has ever been confronted with whether or not the FTC's interpretation of its power under § 45 is proper.

The privacy promises of many websites are problematic when it comes to the sale of Internet company customer lists. Furthermore, much of the information in such lists may not even be compiled with the knowledge or permission of the customer. The claims of privacy and the sensitive nature of the information, which is far more detailed than information in traditional customer lists, could eventually be used to bar any such sale.

While brick and mortar companies have traditionally been able to sell their customer lists, the privacy promises and additional information included in such lists may complicate the sale of similar lists for Internet businesses. As the following section discusses, the sale of e-commerce customer lists has in fact been problematic because of the reasons outlined above.

III. CONFLICT—BANKRUPTCY AND CONSUMER PROTECTION

The conflict between the goals of bankruptcy law and privacy promises came to a head in the now famous *Toysmart.com* case.[211] "[O]ften [customer information] can't be sold because of privacy concerns," despite its great value to creditors.[212] As a result of the great amount of publicity following that case, other Internet

---

210. Wingate, *supra* note 13, at 909.

211. *See infra* Part III.A.

212. Weintraub, *supra* note 13, at 914 (noting, however, "if a bankrupt dot-com acquired personal consumer data without posting a privacy policy, the bankruptcy trustee is obliged to sell the consumer database in order to maximize the liquidation value of the estate.").

companies have dealt with the problem in several ways.[213]

A. Toysmart.com—The Beginning of the Problem

Toysmart.com ("Toysmart") had great potential.[214] It was significantly backed by The Walt Disney Company ("Disney"),[215] which owned a sixty percent stake in the company,[216] and was among one of the most visited websites during the 1999 Christmas season.[217]

As a retailer of children's educational toys,[218] the information Toysmart received about its customers included names, addresses, billing information, purchasing preferences, and information on the children for whom the purchases were made.[219] This information was considered quite sensitive, as it embraced both financial information and information about children.[220] By June 2000, Toysmart had information on over 250,000 customers.[221] Like many other web retailers, Toysmart promised not to share its

---

213. *See infra* Parts III.B–III.E.

214. *See* Miller & O'Rourke, *supra* note 13, at 790 (noting that Toysmart "initially attracted considerable attention and financing"); *see also* Beckmann, *supra* note 21, at 766 (citing magazines such as *U.S. News & World Report*, *Time*, and *Parents* as finding Toysmart among the best online toy retailers).

215. *See* Miller & O'Rourke, *supra* note 13, at 790; *see also* Wingate, *supra* note 13, at 910.

216. *See* Linda Rosencrance, *Toysmart Customers Still In Limbo: States Object to Bankruptcy Settlement that Permits Transfer of Company's Customer List*, PCWORLD.COM, Aug. 4, 2000, *available at* http://www.pcworld.com/news/article.asp?aid=17944 (last visited Mar. 25, 2002); *see also* Joel R. Reidenberg, The Toysmart Bankruptcy, 23rd International Conference of Data Protection Commissioners, Paris (Sept. 24, 2001), *available at* http://www.cnil.fr/conference2001/eng/contribution/reidenberg1_contrib.pdf (last visited Sept. 26, 2002).

217. *See* Rosencrance, *supra* note 216; *see also* Miller & O'Rourke, *supra* note 13, at 790; Reidenberg, *supra* note 216.

218. *See* Miller & O'Rourke, *supra* note 13, at 790; *see also* Wingate, *supra* note 13, at 910.

219. *See* Beckmann, *supra* note 21, at 766; *see also* Reidenberg, *Toysmart*, *supra* note 216; Miller & O'Rourke, *supra* note 13, at 792; Jones & Evans, *supra* note 51; Wingate, *supra* note 13, at 910.

220. *See* Jones & Evans, *supra* note 51.

221. *See* Reidenberg, *supra* note 216; *see also* Beckmann, *supra* note 21, at 766.

information:[222]

> (1) "Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by Toysmart.com is used only to personalize your experience online;" and (2) "When you register with toysmart.com, you can rest assured that your information will never be shared with a third party."[223]

Toysmart also became a member of TRUSTe[224] in September 1999.[225]

However, by 2000, Toysmart had hit upon hard times[226] and ceased operations as of May 19, 2000.[227] Only three days later, May 22, the company started seeking buyers for its assets.[228] Shortly thereafter, on June 8, 2000, Toysmart placed an advertisement in the *Wall Street Journal* to sell its assets, including its customer list.[229]

---

222. *See* Davidson, *supra* note 12; *see also* Miller & O'Rourke, *supra* note 13, at 792; Beckmann, *supra* note 21, at 767.

223. Complaint, ¶ 8, FTC v. Toysmart.com, L.L.C. (D.C. Mass. 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcmp.htm (last visited Mar. 25, 2002) (quoting the Toysmart privacy policy from its website).

224. *See generally supra* note 69 (discussing TRUSTe).

225. *See* Complaint, ¶ 8, *Toysmart*; *see also* Blakeley, *supra* note 13; Wingate, *supra* 13, at 910; *accord* Miller & O'Rourke, *supra* note 13, at 794

226. *See* Wingate, *supra* note 13, at 766 (explaining how Toysmart's 2000 Christmas sales failed to meet expectations and how the company was running out of operating capital and could not raise the necessary funds through an initial public offering because of the failing stock prices of Internet businesses in early 2000); *see also* Miller & O'Rourke, *supra* note 13, at 790–91 (describing how Disney's change in strategy to focus on "entertainment and leisure products" and Toysmart's inability to raise additional funds because of investor fears resulted in Toysmart's downfall).

227. *See* Complaint, ¶ 10, *Toysmart*; *see also* Miller & O'Rourke, *supra* note 13, at 791; Beckmann, *supra* note 21, at 766.

228. *See* Complaint, ¶ 11, *Toysmart*; *see also* Jones & Evans, *supra* note 51; Davidson, *supra* note 12.

229. *See* Keith Dawson, *FTC to Toysmart: Define 'Never,'* INDUS. STANDARD MAG., July 11, 2000, *available at* http://www.technologyfront.com/journalism/2000/07/11.html (last visited Mar. 26, 2002); *see also* Davidson, *supra* note 12; Miller & O'Rourke, *supra* note 13, at 792; Morris & Fearon, *supra* note 13; Beckmann, *supra* note 21, at 767.

The next day, June 9, 2000, Toysmart's creditors filed an involuntary bankruptcy petition.[230]

The sale of the customer list proved to be problematic because it would result in a violation of Toysmart's posted privacy policy.[231] Upon learning of the sale of the Toysmart customer list, the FTC filed suit under 15 U.S.C. § 45 on July 10, 2000, in the District Court of Massachusetts to prevent the sale.[232] Forty-four State Attorneys General also opposed the sale for similar reasons.[233] However, the FTC and Toysmart settled the case, prohibiting the sale of the customer list "as a stand-alone asset."[234] "The settlement only allows a sale of such lists as a package which includes the entire Web site, and only to a 'Qualified Buyer'—an entity that is in a related market and that expressly agrees to be Toysmart's successor-in-interest as to the customer information."[235]

"Toysmart believed that its customer list was worth millions of dollars." Blakeley, *supra* note 13.

230. *See* Complaint, ¶ 12, *Toysmart*; *see also* Miller & O'Rourke, *supra* note 13, at 791; Reidenberg, *supra* note 216; Beckmann, *supra* note 21, at 766.

231. *See* Reidenberg, *supra* note 216.

232. Press Release, Federal Trade Commission, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), *available at* http://www.ftc.gov/opa/2000/07/toysmart2.thm (last visited Jan. 24, 2002) [hereinafter FTC Release II]; *see also* Toysmart Complaint; Jones & Evans, *supra* note 51; Reidenberg, *supra* note 216; Beckmann, *supra* note 21, at 767; Miller & O'Rourke, *supra* note 13, at 792–93; Blakeley, *supra* note 13; Wingate, *supra* note 13, at 910. Notably, the FTC would not have been able to step in if Toysmart did not have a privacy policy. *Accord* Davidson, *supra* note 12.

233. *See* Reidenberg, *supra* note 216; *see also* Miller & O'Rourke, *supra* note 13, at 792; Morris & Fearon, *supra* note 13; Blakeley, *supra* note 13.

234. FTC Release II, *supra* note 232; *see also* Miller & O'Rourke, *supra* note 13, at 793; Beckmann, *supra* note 21, at 767. At least one person believes that by settling with Toysmart, "the FTC has demonstrated that it remains unsure of its preferred legal standard." Wingate, *supra* note 13, at 908.

235. *See* FTC Release II, *supra* note 232; *see also* Reidenberg, *supra* note 216 ("Essentially, the term [Qualified Buyer] was defined as a company in the same type of business . . .that would agree to Toysmart's commitments for the treatment of the personal information."); Miller & O'Rourke, *supra* note 13, at 793; Davidson, *supra* note 12; Wingate, *supra* note 13, at 911; Beckmann, *supra* note 21, at 766; Blakeley, *supra* note 13 (stating that "[t]he creditors' committee of Toysmart objected to the settlement . . . complaining that the settlement would chill bidding."); Beckmann, *supra* note 21, at 769 (noting that Toysmart creditors

According to the settlement, the Qualified Buyer has to either follow the Toysmart privacy policy or provide notice and obtain permission from each of the persons on the list if the buyer were to change the terms outlined in the Toysmart privacy statement.[236] The settlement also required Toysmart to destroy the list if a Qualified Buyer did not come forward.[237]

Not all FTC officials were satisfied by the settlement. Two FTC Commissioners voted against the settlement.[238] In a dissenting statement, Commissioner Orson Swindle stated:

> I do not think that the Commission should allow the sale. If we really believe that consumers attach great value to the privacy of their personal information and that consumers should be able to limit access to such information through private agreements with businesses, we should compel businesses to honor the promises they make to consumers to gain access to this information. Toysmart promised its customers that their personal information would *never* be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because "never" really means never.[239]

Similarly, Commissioner Sheila F. Anthony stated:

> To accept the bankruptcy settlement would place business concerns ahead of consumer privacy. Although the proposed settlement's definition of a qualified buyer attempts to ensure that only an entity "similar" to Toysmart is eligible to purchase the list, I do not believe that this limitation is an adequate proxy for consumer privacy interests. In my view, consumer privacy would be better protected by requiring that consumers themselves be given notice and choice before their detailed personal information is shared with or used by another

---

objected to the settlement with the FTC because it would limit their abilities to maximize the value of the assets because no buyer had been located).

236. *See generally* sources cited *supra* note 235.

237. *See generally* sources cited *supra* note 235.

238. FTC Release II, *supra* note 232; *see also* Miller & O'Rourke, *supra* note 13, at 793–94; Wingate, *supra* note 13, at 911–12.

239. Orson Swindle, Dissenting Statement, *available at* http://www.ftc.gov/os/2000/07/toysmartswindlestatement.htm (last visited Mar. 25, 2002) (emphasis in original).

> corporate entity – especially where, as here, consumers provided that information pursuant to a promise not to transfer it.[240]

Despite the agreement between the FTC and Toysmart, forty-six attorneys general[241] opposed the settlement because it violated the consumer protection laws of their respective states and did not give consumers the option to opt-in.[242] New York and Texas filed separate objections.[243] The states had jurisdiction because "the privacy promise extended to consumers within each of the respective states."[244]

The settlement and the states' objections to the settlement proved to be irrelevant, as the bankruptcy court refused to accept the settlement proposal.[245] "Under the terms of [the] ruling, any

---

240. Sheila F. Anthony, Dissenting Statement, *available at* http://www.ftc.gov/os/2000/07/toysmartanthonystatement.htm (last visited Mar. 25, 2002).

241. These states and territories were: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, the Northern Mariana Islands, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Vermont, the U.S. Virgin Islands, Virginia, West Virginia, Wisconsin, and Wyoming. *See* Objection, *In re* Toysmart.com LLP, (D.C. Mass. 2000), *available at* http://www.ago.state.ma.us/oppositi.pdf (last visited Mar. 26, 2002).

242. *See* Reidenberg, *supra* note 216.

> One solution proposed by the state attorney generals in Toysmart.com was to allow debtors to sell their customer lists encumbered by privacy guarantees on e-mail notice to all potentially affected customers and effect consent by such customers, i.e., on an "opt-in" basis. E-mail notice, in a form approved by the bankruptcy court, would not only provide each customer with information regarding a change in circumstance or a change in the original contract it entered with the dot-com, but would also comport with due process requirements that notice be given to any party having an interest in property being sold . . . [e]-mail consent by consumers on an opt-in basis allows the customer to assent to the sale and to enter a new contract at their choosing with the debtor or its successor.

Morris & Fearon, *supra* note 13; *see also* Beckmann, *supra* note 21, at 768–69.

243. *See* Rosencrance, *supra* note 216.

244. *See* Reidenberg, *supra* note 216.

245. *See* Gary H. Anthes, *Toysmart, FTC Overruled on Sale of Customer Data,*

specific offer to sell the data [would] have to go back to the court for approval."[246] The court ultimately did not have to evaluate any buyer for the customer list as Toysmart withdrew it from sale due to low bids[247] and the great public outcry.[248] Instead, the customer list was purchased by Disney for $50,000, with the understanding that the list was to be destroyed.[249]

The FTC is still actively watching the sale of customer lists.[250] According to one FTC official, "In deciding whether to block a data sale, the FTC—and state attorneys general who also monitor these situations—consider a number of factors: Is the data being sold to a company in a similar business? Is it being sold as a stand-alone list or is it part of a broader asset sale? What information is being sold?"[251] However, the FTC has yet to determine a definitive set of rules about whether to block the sale of customer lists because of privacy considerations.[252] Nonetheless, "in the [*Toysmart*] case, the FTC established a possible framework for transferring otherwise confidential customer information to successor-in-interest under certain circumstances."[253]

COMPUTERWORLD, Aug. 17, 2000, *available at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48699,00.html (last visited Sept. 26, 2002); *see also* Reidenberg, *supra* note 216; Morris & Fearon, *supra* note 13; Blakeley, *supra* note 13; Beckmann, *supra* note 21, at 769–70.

246. *See* Reidenberg, *supra* note 216.

247. *See* Miller & O'Rourke, *supra* note 13, at 794. There were rumors, however, that at least one party was willing to pay up to $100,000 for the customer list. *See* Reidenberg, *supra* note 216.

248. *See* Reidenberg, *supra* note 216.

249. *See id.; see also* Miller & O'Rourke, *supra note* 13, at 794; Blakeley, *supra* note 13; Davidson, *supra* note 12.

250. *See* Troy Wolverton, *Egghead Sale Could Crack on Privacy Issue*, CNET NEWS.COM, Aug. 24, 2001, *available at* http://news.com.com/2100-1017-272130.html?legacy=cnet (last visited Jan. 24, 2002).

251. Joelle Tessler, *Bankrupt Dot-coms Ask to Sell User Data*, SILICONVALLEY.COM, Oct. 28, 2001 (citing the statements of Joel Winston, then FTC Acting Associate Director for Financial Practices), *available at* http://www.siliconvalley.com/docs/news/depth/list102901.htm (last visited Jan. 24, 2002).

252. *See* Wingate, *supra* note 13, at 912 ("Evidently, the FTC has not conclusively determined what must be done when a bankrupt e-business attempts to sell personal consumer information in violation of its own privacy policy.").

253. *Id.* at 911.

Toysmart demonstrates that the lack of specific consumer privacy legislation has not barred the enforcement of privacy policies. Rather, "despite the lack of general privacy legislation in the United States, the case illustrates that in exceptional circumstances other consumer protection statutes [namely 15 U.S.C. § 45], may be available to assure the fair treatment of personal information."[254] The public interest in this area and the regulatory powers vested in the FTC have been enough to curtail privacy abuses, despite the lack of court affirmation of the FTC's interpretation of its authority.[255]

In addition, *Toysmart* has demonstrated of the strong public interest in the subject of consumer privacy protection, specifically on the part of state governments.[256] The fact that almost all states objected to the sale of the Toysmart customer list[257] suggests that the concern about consumer privacy is nationwide. "Without the aggressive pursuit of the case by the coalition of states . . . the outcome is likely to have been quite different"[258] as the extent of coordination and cooperation necessary to prevent the sale may not have existed.[259]

As a result of the Toysmart case, many other Internet retailers have opted to treat their customer lists differently in bankruptcy.[260] Still others that remain in business have altered their privacy provisions accordingly.[261]

---

254. Reidenberg, *supra* note 216; *see also* FTC v. Colgate-Palmolive Co., 380 U.S. 374, 384 (1965) ("This statutory scheme [proscribed by 15 U.S.C. § 45] gives the Commission an influential role in interpreting § 5 [of the FTCA] and in applying it to the facts of particular cases arising out of unprecedented situations.").

255. *See supra* note 201 (noting that the *Colgate-Palmolive* Court acknowledged that the FTC is in a better position to determine whether an activity is deceptive or not).

256. *See* Reidenberg, *supra* note 216.

257. *See supra* notes 233, 242–43 and accompanying text.

258. *See* Reidenberg, *supra* note 216.

259. *See id.* (noting that the coordination and cooperation necessary may not be "easy to maintain in future cases").

260. *See infra* Parts III.B–III.D.

261. *See infra* Part IIII.E.

B. No Sale

When Craftshop.com filed for bankruptcy in May 2000,[262] the company tried to sell its customer list.[263] However, the company was challenged by the Texas Attorney General's Office,[264] and opted not to sell the list because the cost of litigating for the right to sell it was higher than the price the list would fetch.[265] As a result, consumer confidentiality was protected and privacy promises were kept, but the value of the bankruptcy estate was decreased by the decision not to sell the customer list. This decision was disadvantageous to Craftshop's creditors and investors and only considered their interests to the extent that the cost of the litigation would decrease the value of the bankruptcy estate more than not selling one of their greatest assets.

C. Opt-Out

Many companies decided to use an opt-out policy, allowing individuals who specifically request to have their names removed to choose not to be included in the sold customer lists.[266] For example, when Living.com declared bankruptcy, the Texas Attorney General's Office opposed the sale of the customer list, seeking an injunction from the bankruptcy court to prevent the sale.[267] The Attorney General's Office and Living.com reached a settlement whereby:

---

262. *See* Greg Sandoval, *Failed Dot-Coms May Be Selling Your Privacy Information*, CNET NEWS.COM, June 29, 2000, *available at* http://news.com.com/2100-1017-242649.html?legacy=cnet (last visited Mar. 26, 2002).

263. *See* Davidson, *supra* note 12.

264. The Texas Attorney General's Office has "built . . . a reputation for stalking listsellers," causing many to give up on the endeavor. *Id.*

265. *See id.*

266. *See* Piera, *supra* note 178, at 14.

267. *See* Press Release, Office of the Attorney General, State of Texas, Cornyn Announces Privacy Settlement with Living.com—Protects Texans Privacy Rights (Sept. 25, 2000), *available at* http://www.oag.state.tx.us/newspubs/releases/2000/20000925living.com.htm (last visited Mar. 26, 2002).

> The court-appointed bankruptcy trustee will oversee the destruction of the customers' personal financial data such as credit card, bank account and social security numbers. While the bankruptcy trustee may sell or transfer the customer list-excluding credit card, bank account and social security numbers—she may do so only after giving notice to all of living.com's customers and giving the consumers an opportunity to opt-out of the proposed sale.[268]

The bankruptcy court approved the settlement[269] and the list was ultimately sold to Martha Stewart Living Omnimedia and the Maxwell Sroge Company for $100 per 1,000 names.[270]

When Voter.com went out of business,[271] it sought to sell its subscriber list, including email addresses, party affiliations, issues of interest to the users, gender data, and zip codes, but not names or addresses. [272] Voter.com decided to sell its list only to buyers who would use it for the same purpose it had.[273] The company also promised to contact every person on the list and give them the chance to opt-out.[274] However, Voter.com did hope to sell its list to up to four different buyers.[275] It has not been reported who purchased Voter.com's subscriber information or under what terms.

When Egghead.com filed for bankruptcy, its bankruptcy judge

---

268. *See id.*; *see also* Davidson, *supra* note 12.

269. *See* Susan Stellin, *Dot-Com Liquidations Put Consumer Data in Limbo*, N.Y. TIMES, Dec. 4, 2000, at C4.

270. *See* Davidson, *supra* note 12.

271. *See* David McGuire, *Privacy Advocates Question Voter.com's Subscriber List Sale*, NEWSBYTES, Sept. 16, 2001, *available at* http://www.infowar.com/class_1/01/class1_031601a_j.shtml (last visited Sept. 26, 2002).

272. *See* Aaron Pressman, *Voter.com to Sell Membership List*, INDUS. STAND., Mar. 15, 2001, *available at* http://www.thestandard.com/article/0,1902,22894,00.html (last visited Jan. 24, 2002).

273. *See* McGuire, *supra* note 271.

274. *See* Pressman, *supra* note 272 (noting, however, that privacy advocates were still concerned that the sale of the list could result in misuse if it were sold to partisan groups that the subscribers disagreed with).

275. *See id.*; *see also* McGuire, *supra* note 271.

indicated that an opt-out policy was not required.[276] Egghead.com nonetheless tried to use the opt-out option to avoid any privacy challenges in a sale deal with Fry's Electronics ("Fry's").[277] Fry's required that no more that ten percent of active users, defined as buyers having made a purchase on Egghead.com in the past two years, opt-out.[278] Fry agreed not to disclose the customer data upon receipt.[279] The ten percent requirement gave great leveraging power in their bargaining with Egghead.com; if the terms were not met, Fry's could use the fact to lower the price.[280] On the other hand, such terms undermine attempts to maximize the bankruptcy estate.[281] The deal ultimately fell apart and Egghead.com's assets were acquired by Amazon.com, which agreed to honor Egghead.com's privacy policy.[282]

Unlike Egghead.com and Voter.com, More.com saw the writing on the wall and eased its privacy policy before selling its customer list.[283] Purchaser HealthCentral.com did not obtain either the health data or shopping histories of the customers on the list and offered $25 off to customers remaining on the list after an opt-out option was extended.[284] No regulatory action was taken against More.com.[285]

Despite the risk that lists purchased with opt-out options may not have as many names as the original customer lists,[286] many companies have nonetheless purchased these lists. W. Atlee Burpee & Co. bought the Garden.com customer list, after listees had a chance to opt-out, in an attempt to attract younger

276. *See* Tessler, *supra* note 251.

277. *See* Wolverton, *supra* note 250 (noting that Fry believed that the opt-out provision would protect consumer privacy).

278. *See id.*

279. *See id.*

280. *See id.*

281. *See supra* Part I.A.

282. *See* Alorie Gilbert, *Egghead.com Bounces Back Under Amazon*, CNET NEWS.COM, Dec. 18, 2001, *available at* http://news.com.com/2100-1017-277185.html?legacy=cnet (last visited Mar. 26, 2002).

283. *See* Davidson, *supra* note 12.

284. *See id.*

285. *See* Beckmann, *supra* note 21, at 790.

286. *See* Tessler, *supra* note 251.

customers.[287] Similarly, eVineyards bought Wine.com's customer list after an opt-out option because a certain amount of customer information had to be turned over in order to honor Wine.com's many outstanding orders and gift certificates.[288]

In response to the *Toysmart* case, many companies have chosen to give people on customer lists the chance to opt-out. In some cases, more sensitive information was not disclosed; in other cases, the lists could only be sold to parties with similar goals as the selling party. Still other companies have eased their policies, along with using opt-out, to keep the sales from being stopped. Opt-out has not stopped buyers from being interested in customer lists, as the lists allow purchasers to target different types of customers or because the nature of the sales required that a certain amount of information be transferred. However the opt-out "provision that is meant to reassure customers about their privacy ends up being something that devalues a key asset of the company, which is its customer list."[289] At least one company has limited the amount of customers that can opt-out to ensure that the list is not worthless because too many people have opted-out.[290]

D. Opt-In

Other defunct Internet businesses have granted even more privacy to their subscribers, selling customer lists after the listees decide to opt-in, where all of the people on the list specifically

---

287. Weintraub, *supra* note 13. As the terms of the sale were not disclosed, it is unclear which, if either party, requested the opt-out option. *See* Moira Cotlier, *Market in Bloom*, CATALOG AGE, Apr. 2001.

288. *See* Tessler, *supra* note 251 (citing eVineyard's Chief Marketing Officer Brett Lauter). Of the customer names purchased, approximately 30% were discarded because eVineyard did not believe it could legally ship alcohol to customers in certain states. *See* Thane Peterson, *E-Cheers from Larry Gerhard: The eVineyard.com CEO's Conservatism Has Kept the Company Flowing As Other Wine-Selling Dot-Com's Dried Up. How He's Thinking Big*, BUSINESS WK. ONLINE, July 17, 2001. It is unclear whether either Wine.com or eVineyard was responsible for the decision to give customers the choice to opt-out.

289. Wolverton, *supra* note 250 (quoting attorney Rick Gray).

290. *See supra* note 278 and accompanying text (discussing how Fry would only purchase the Egghead.com customer list if less than ten percent of the customers opted out).

indicate that they would like their information to be shared.[291] "In some sense, what many of these companies are trying to do is amend the privacy policies they had in place when they were still in business."[292] By asking for permission to sell the information, the companies are remaining within the privacy promises they made.[293] In the case of eToys.com, a complaint by the Texas Attorney General before the eToys bankruptcy court resulted in a settlement requiring the list, ultimately sold to KB Toys, to be subject to opt-in.[294]

However, when Webvan.com went out of business, WhyRunOut.com was willing to buy its customer list after those on the list chose to opt-in because "while we're not getting 100 percent of their list . . . the ones we aren't getting are the ones who aren't interested in our service anyway."[295] In the end, WhyRunOut.com got less than ten thousand names from the customer list,[296] a fraction of the 160,000 Webvan users as of July 2000.[297]

Opt-in essentially solves the problem of violating privacy promises to increase the value of customer lists because although a promise initially existed, it is replaced by a second agreement, allowing the transfer of the information.

E. Changes in Privacy Policy

Following the *Toysmart* case, which emphasized the conflict

---

291. *See* Piera, *supra* note 178, at 14.

292. *See* Tessler, *supra* note 251 (quoting technology law attorney Patrick Guevara).

293. *See id.*

294. *See* Press Release, Office of the Attorney General, State of Texas, Cornyn Victorious in "eToys" Case—Privacy Protection Action Secures Rights of 3 Million Online Customers (May 18, 2001), *available at* http://www.oag.state.tx.us/newspubs/releases/2001/20010518etoys2.htm (last visited Mar. 26, 2002).

295. Tessler, *supra* note 251 (quoting WhyRunOut.com's Chief Executive Officer Dan Frahm).

296. *See id.*

297. *See Webvan's Loss Widens as Company Expands*, USATODAY.COM, July 13, 2000, *available at* http://www.usatoday.com/life/cyber/invest/in872.htm (last visited Apr. 20, 2002).

between maximizing bankruptcy estates and protecting consumer privacy (and ensuring that companies abide by their privacy promises), some companies simply changed their privacy policies to allow for disclosure of customer lists upon sale.[298] For example, Amazon.com changed its privacy policy because of *Toysmart*[299] to include a section entitled "Business Transfers," which states:

> As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.[300]

Amazon believes that the new policy actually affords customers greater protection. Patty Smith, one of Amazon's representatives, says "the privacy policy is actually stricter now because it promises not to sell data except in certain instances."[301]

Likewise, eBay.com altered its privacy policy in response to *Toysmart*.[302] The relevant part of the policy now states:

> It is possible that eBay, its subsidiaries, its joint ventures, or any combination of such, could merge with or be acquired by another business entity. Should such a combination occur, you should expect that eBay would share some or all of your information in order to continue to provide the service. You will receive notice of such event (to the extent it occurs) as provided in Section 11 ("Notice") and we will require that the new combined entity follow the practices disclosed in this

298. *See* Jeffery Benner, *eBay Alters Privacy Policy*, WIRED NEWS, Apr. 2, 2001, *available at* http://www.wired.com/news/business/0,1367,42778,00.html (last visited Mar. 26, 2002); *see also* Miller & O'Rourke, *supra* note 13, at 836.

299. *See* Beckmann, *supra* note 21, at 788; *see also* Wolverton, *supra* note 250; Reidenberg, *Toysmart*, *supra* note 216; Miller & O'Rourke, *supra* note 13, at 836–37; Blakeley, *supra* note 13; Davidson, *supra* note 12.

300. Amazon.com Privacy Notice, *at* http://www.amazon.com/exec/obidos/tg/browse/-/468496/002-4154388-1678443 (last visited Sept. 19, 2002).

301. Davidson, *supra* note 12.

302. *See* Benner, *supra* note 298; *see also* Reidenberg, *supra* note 216; Miller & O'Rourke, *supra* note 13, at 836–37.

Privacy Policy.[303]

If the eBay list were sold, customers or consumer protection groups may still be able to challenge the sale of the list if the successor company fails to abide by the eBay privacy policy. However, it is unclear whether any buyer would be willing to risk litigation or conflict[304] instead of simply paying a lower price for the diminished value of the list.

As stated above, one simple solution to the *Toysmart* problem has simply been to change privacy policies to allow disclosure of customer information upon sale, merger, or acquisition. These changes in privacy policy "preclude any future action for 'unfair or deceptive' practices and diminish the level of privacy protection afforded to consumers in the case of corporate bankruptcies."[305] Rather, customer lists could simply be sold because there is no law (bankruptcy or otherwise) that would bar the sale.[306] "In the future, many companies are unlikely to have any such privacy policy that would offer consumers or state prosecutors the opportunity to challenge the disposition of personal information in a bankruptcy."[307] If most Internet businesses change their policies in a similar manner, the *Toysmart* problem could simply go away, leaving consumers unprotected when customer lists are sold

303. eBay Privacy Policy, *at* http://pages.ebay.com/help/community/png-priv.html (last visited Sept. 20, 2002).

304. Certainly, other companies, such as Craftshop.com, Voter.com, More.com and WhyRunOut.com, have been willing to better abide by their own privacy promises in order to prevent the sale of customer lists from being challenged. *See supra* Parts III.B–III.D.

305. Reidenberg, *supra* note 216. However, one could argue that by altering the privacy policy, it only applies to new customers, not to those who made purchases under the old policy. *See* Robert L. Eisenbach III, *The Internet Company's Customer List: Asset or Liability?*, COMPUTER & INTERNET LAW, Aug. 2001, at 25. "If a company wants the old customer information to be governed by its new privacy policy, it may be required to alert each customer of the change and give the customer the opportunity to choose whether or not they want their information governed by the new privacy policy." *Id.* (citing TRUSTe Model Privacy Statement).

306. *See* Miller & O'Rourke, *supra* note 13, at 837.

307. Reidenberg, *supra* note 216.

because of bankruptcy.[308]

F. When Is the Problem Less Problematic?

The *Toysmart* problem, however, is not as relevant if the Internet business is acquired or merged, instead of going through bankruptcy or going out of business[309] because "[w]hen a company declares bankruptcy, all bets are off."[310] A bankruptcy judge can declare contracts void to maximize the value of the estate.[311]

However, when a company is acquired or merged, the purchaser is essentially a successor-in-interest and is bound by the privacy promise.[312] A merger is the absorption of one company by another, where the surviving corporation obtains all the assets, liabilities and powers of the acquired company.[313] Where one company buys substantially all the assets of another company, as opposed to purchasing the stock of the company to be acquired, courts will hold that the acquisition is a de facto merger and impose successor liability.[314] "[A]s a general rule, in the bricks-and-mortar world, the assignment of substantially all assets of one company to a new company binds that new company to the obligations of the former company."[315]

---

308. *See* Beckmann, *supra* note 21, at 790 ("The only logical response from the [e-commerce] industry would be to lower the standard of privacy practices to resemble Amazon's new approach.").

309. *See* Manny Madriaga, *A Treasure Hunt Among the Dot-Com Ruins*, *available at* http://www.iploft.com/articles3.htm (last visited Sept. 27, 2002); *see also* Tessler, *supra* note 251.

310. Tessler, *supra* note 251 (quoting TRUSTe spokesman David Steer).

311. *See id.* (quoting TRUSTe spokesman David Steer).

312. *See* Linda Rosencrance, *Sale of More.com's Customer List Raises Privacy Concerns*, CNN.COM, Oct. 27, 2000, *available at* http://www.cnn.com/2000/TECH/computing/10/27/online.privacy.idg/ (last visited Sept. 27, 2002).

313. *See* Douglas R. Richmond, *Products Liability: Corporate Successors and the Duty to Warn*, 45 BAYLOR L. REV. 535, 554 (1993).

314. *See* J. Maxwell Tucker, *The Clash of Successor Liability Principles, Reorganization Law, and the Just Demand That Relief Be Afforded Unknown and Unknowable Claimants*, 12 BANKR. DEV. J. 1, 11 (1995).

315. Rosencrance, *supra* note 312 (quoting Pennie & Edmonds attorney Jonathan Moskin).

Likewise, a "[c]onsolidation occurs where two or more constituent corporations consolidate and a single new corporation is created. The prior constituents cease to exist following consolidation. The new, successor corporation assumes the assets and liabilities of its constituents."[316]

Whether the acquisition amounts to a merger or consolidation, the surviving company assumes the liabilities of the predecessor company or companies.[317] The underlying theory for successor liability is that the old company did not cease to exist, "but merely directed the blood of the old corporation into the veins of the new."[318] The successor liability rule is a cornerstone of corporate law that is generally codified.[319]

As a result, when defunct Internet companies are merged or acquired by other entities, the acquirer assumes the liabilities of the old company, including the privacy promises.[320] This assumption of liability is generally enough to satisfy the FTC that customer data will be adequately protected.[321] However, in bankruptcy, where assets are sold off piece by piece, the liabilities are not passed to the purchaser, so that the seller is essentially violating its own privacy policy.

---

316. Richmond, *supra* note 313, at 554.

317. *See id.* at 554.

318. *Id.*

319. *Id.*

320. While the transmission of a customer list as part of a merger or acquisition could still technically constitute a violation of a privacy policy, it is unlikely to be challenged because the successor in interest is bound to the original terms of the privacy policy. *See supra* note 251 and accompanying text (discussing how the FTC considers whether a list is being sold to a similar company, whether it is being sold as part of a larger sale or individually, and what information is being sold when deciding whether to challenge the sale). However, this fails to consider a situation in which a small, local business is taken over by a large, national "mega-company." While the sale could require the buyer to abide by the seller's existing privacy policy in such a sale, the extreme difference in size between the two companies, and therefore their abilities to exploit such information, could in itself constitute a breach of the promise. Given that challenging the sale of customer lists is quite recent, no one has either opposed a sale for this reason or undertaken an academic discourse on the subject.

321. *See supra* note 251 and accompanying text; *see also supra* Part III.A (discussing the *Toysmart* settlement).

IV. RESOLUTION

A. Policy Interests Regarding Customer Lists in E-Commerce

There are certain policy interests that must be considered when discussing the sale of customer lists from failed Internet businesses. While the use of the Internet is growing,[322] the Internet will not reach its full potential if consumers fear that their privacy will not be protected.[323] Any consideration of policy interests must be aimed at maximizing economic return and consumer sales while at the same time addressing the legitimate privacy concerns of users. Essentially, companies should be able to sell to interested customers and said customers should feel safe entering into such transactions.

Secondly, when discussing online privacy and customer lists, one must remember that many Internet companies receive financing through venture capital investment.[324] The burst of the Internet bubble does not mean that all investment in Internet companies is over.[325] While venture capitalism is not without risks, an investor's loss can be minimized by maximizing the value of assets of a failed company.[326] If customer lists are barred from sale or subject to litigation, leaving little else of value in the estate of the failed company, investing companies may opt to place their money in safer, less unstable ventures.[327] As a result, investment in Internet companies could diminish further, reducing consumer convenience, competition, and economic growth in the retail sector.

---

322. *See supra* Part II.A.

323. *See* Beckmann, *supra* note 21, at 770.

324. *See* Wingate, *supra* note 13, at 915–16 (indicating that venture capitalists are still willing to invest in start-ups, despite the Internet bubble burst).

325. *See id.* at 916 ("Many venture capitalists declare that they will continue to invest heavily in the development of e-commerce.").

326. *Accord id.* at 917–18 (noting that venture capitalists have shifted some funds from Internet companies to the telecommunications industry in part because of the ability of failed telecom companies to sell their bandwidth, allowing the venture capital company some degree of recovery).

327. *See id.* at 918.

B. Proposed Legislation to Protect Consumers

After the *Toysmart* fiasco, much legislative attention was given to the problem of selling customer lists protected by privacy promises.[328] Below is a brief explanation of proposed legislation, with a focus on the pending Bankruptcy Reform Act of 2001.

1. The Online Privacy Protection Act of 2001

The purpose of H.R. 89, also known as the Online Privacy Protection Act of 2001, is:

> To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes.[329]

Such regulations must require webpage operators to clearly post a notice indicating what information is collected, allow users to limit the use of the information or consent to its use for non-transactional purposes, and require that webpage operators to establish procedures for protecting information.[330]

Thus H.R. 89 gives the FTC the power to require all companies to allow users to limit the use of their information, even if the users would have willingly done business with the company without a privacy policy. As a result, customer lists and their monetary value to buyers could be curtailed in situations where lists could have been compiled and sold without any objections from website users.

---

328. *See* Reidenberg, *supra* note 216 ("A second trend [resulting from *Toysmart*] is the legislative effort to revise the bankruptcy code."); *see also* Miller & O'Rourke, *supra* note 13, at 839.

329. Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001), *available at* http://www.steptoe.com/webdoc.nsf/Files/HR89/$file/HR89.pdf (last visited Mar. 28, 2002).

330. *Id.*

Moreover, H.R. 89 does not expressly prohibit the sale of customer information; its main focus is on ensuring that customers are informed about how their information is used. As such, it does not necessarily resolve the *Toysmart* problem, as it does not bind companies to uphold their privacy promises. Companies can simply alter their policies to allow for disclosure upon sale.[331]

2. The Consumer Internet Privacy Enhancement Act

The Consumer Internet Privacy Enhancement Act, H.R. 237, is intended to protect the privacy of Internet customers.[332] Like the Online Privacy Protection Act, the Consumer Internet Privacy Enhancement Act requires web operators to provide notice and allow consumers to limit the use of such information.[333] However, H.R. 237 does not empower the FTC to dictate the terms of collecting consumer data; rather it explicitly makes the collection of such information without notice and the opportunity to opt-out illegal.[334] As with the Online Privacy Protection Act, H.R. 237 forces companies to provide a limitation for the uses of consumer information though the company would rather simply have no privacy policy and it does not resolve the *Toysmart* issue because companies may simply alter their policies to allow for the sale of customer lists.

3. The Consumer Online Privacy and Disclosure Act

The Consumer Online Privacy and Disclosure Act, H.R. 347,[335] is essentially a combination of the Online Privacy Protection Act and the Consumer Internet Privacy Enhancement Act. It requires the FTC to draft privacy rules and also makes the collection of

331. *See supra* Part III.E.

332. Consumer Internet Privacy Enhancement Act, H.R. 237, 107th Cong. (2001), *available at* http://www.wow-com.com/pdf/hr237introeshoo.pdf (last visited Mar. 28, 2002).

333. *See id.*

334. *Id.*

335. Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001), *available at* http://www.wow-com.com/pdf/hr347introgreen.pdf (last visited Mar. 28, 2002).

consumer data illegal without notice and opt-out opportunities.[336] As with previously discussed legislation, it forces privacy policies upon Internet companies and does not directly resolve the *Toysmart* problem, for the reasons outlined above.[337]

4. The Privacy Policy Enforcement in Bankruptcy Act of 2000

The Privacy Policy Enforcement in Bankruptcy Act, S. 2857, seeks to amend the Bankruptcy Code to exclude personally identifiable information from the assets of a debtor.[338] This legislation seeks to create a new § 541(b)(6) in the Bankruptcy Code, which would state: "(6) if the sale or disclosure of personally identifiable information violates a privacy policy of the debtor in effect at the time at which such information was collected, such personally identifiable information."[339] This act force sites to honor their privacy policies but does not require consumer consent for the sale of information[340] and would simply result in Internet businesses changing their privacy policies like Amazon and eBay did in the wake of *Toysmart*.[341]

5. The Consumer Privacy Protection Act

The Consumer Privacy Protection Act, S. 2606, like much of the aforementioned legislation, requires that customers be given notice about a site's privacy policy.[342] Similarly, the Consumer Privacy Protection Act requires that web page operators obtain affirmative consent from customers before collecting personally

336. *Id.*

337. *See supra* Part IV.B.1.

338. *See* Privacy Policy Enforcement in Bankruptcy Act of 2000, S. 2857, 106th Cong. (2000); *see also Leahy: New Senate Bill Would Enforce Privacy Policies of Firms in Bankruptcy, Plugging "The Toysmart Loophole,"* U.S. NEWSWIRE, July 12, 2000.

339. Privacy Policy Enforcement in Bankruptcy Act of 2000, S. 2857, 106th Cong. (2000).

340. *See* Miller & O'Rourke, *supra* note 13, at 841.

341. *See* Beckmann, *supra* note 21, at 789; *see also* Miller & O'Rourke, *supra* note 13, at 841 ("If the market continues to move to privacy policies that authorize sale, this legislation would effectively be a dead letter.").

342. Consumer Privacy Protection Act, S. 2606, 106th Cong. § 102(a) (2000).

identifiable information.[343] Additionally, S. 2606 removes personally identifiable information from a debtor's assets by amending the Bankruptcy Code.[344] By doing so, the Consumer Privacy Protection Act precludes creditors of failed Internet businesses from obtaining the maximum return on their losses by prohibiting the sale of one of the debtor's most valuable assets—it's customer list.[345] While this legislation would solve the *Toysmart* problem, it would be problematic from a bankruptcy standpoint, as creditors could not realize even a fractional return on their losses.[346] This could discourage or prevent companies from investing in Internet businesses. Moreover, it dictates that companies not sell certain information that they might otherwise be able to because the company would not have opted to use a privacy policy as a term of conducting business with a consumer.[347]

6. The Bankruptcy Reform Act of 2001

The Bankruptcy Reform Act of 2001, S. 420 and H.R. 333, seeks to amend the bankruptcy code to include customer lists within the definition of property and to require a separate hearing to sell non-public personal information protected by a privacy promise at the time of the bankruptcy filing.[348] To this end, if the trustee wishes to sell such information, she must request the court to appoint an ombudsman.[349]

---

343. *Id.* § 102(b).

344. *Id.* § 601.

345. *See* Beckmann, *supra* note 21, at 789.

346. *See id.* at 791 (stating that "this bill would cripple the online direct marketing industry.").

347. *See id.*

348. *See* Bankruptcy Reform Act of 2001, S. 420, 107th Cong. § 231 (2001); *see also* Bankruptcy Reform Act of 2001, H.R. 333, 107th Cong. § 231 (2001). Because the relevant sections of S. 420 and H.R. 333 are identical and for the sake of ease, the remainder of this discussion will cite only to the Senate version.

349. *See* Bankruptcy Reform Act of 2001, S.420, 107th Cong. § 232(a)(1) (2001).

> It shall be the duty of the ombudsman to provide the court information to assist the court in its consideration of the facts, circumstances, and conditions of the sale or lease under section 363(b)(1)(B) of title 11, United States Code, as amended by this Act. Such information may include a presentation of the debtor's privacy policy in effect, potential losses or gains of privacy to consumers if the sale or lease is approved, potential costs or benefits to consumers if the sale or lease is approved, and potential alternatives which mitigate potential privacy losses or potential costs to consumers.[350]

The Bankruptcy Reform Act does not expressly forbid the sale of customer lists but simply formalizes the use of a balancing test similar to the one the FTC currently uses.[351] However, the test is employed by the bankruptcy courts, not the FTC, which could simply allow the sale, "with or without conditions."[352] Aside from the recommendations of the ombudsman, which the court is not bound by,[353] a bankruptcy judge considers both the interests of the customers whose data is compiled and the interests of the creditors. Presumably, this would allow the sale of information not covered by a privacy policy. However, S. 420 does not establish explicit rules for allowing and disallowing such sales, which could potentially lead to inconsistencies.[354] Moreover, because of its broad language, it will take courts some time to create precedent.

What may be more frightening is that the legislation could simply allow Internet companies to change their privacy policies immediately preceding bankruptcy filings.[355] "[I]f the policy is not in effect when the petition is filed the protective provision ostensibly does not apply."[356] Additionally, by amending the Bankruptcy Code to include customer lists within the definition of property, the amendment renders irrelevant any outside

---

350. *Id.* § 232(a)(B)(2).

351. *See supra* note 251 and accompanying text.

352. *See* Miller & O'Rourke, *supra* note 13, at 844.

353. *See id.* at 845 ("[T]he court is free to reject whatever recommendation the ombudsman makes.").

354. *See id.* at 845 (indicating that S. 420 "would create a good deal of uncertainty for both consumers and creditors").

355. *See id.* at 844.

356. *See id.*

interpretation considering such lists to be contacts subject to enforcement.[357]

7. Pending State Legislation

Aside from the above-mentioned legislation, there are currently hundreds of bills pending in state legislatures across the country.[358] Because the of the easy access to the Internet and the fact that online companies are doing business in every state in the nation, "the most restrictive of the state laws will become the de facto national standard."[359] Given the nationwide (and global) implications of Internet business and technology, a federal solution seems far more appropriate.[360]

C. Third Party Customer Information Management

One other solution that has been implemented because of growing concern about the sale of customer data has been to allow third parties to own and manage consumer data.[361] While such an arrangement simply does away with the conflict, it does not allow companies to use their lists as collateral, which in turn limits their ability to get financial backing.[362] Furthermore, if Internet companies no longer have their customer lists, their assets at bankruptcy are likely to be quite limited. There may be very little else of value to settle debts with creditors.

D. An Academic Solution

Professor Walter W. Miller and Maureen A. O'Rourke of the Boston University School of Law have proposed yet another solution.[363] They suggest a two prong solution requiring that (1) websites provide explicit (and conspicuous) privacy notices,

357. *See id.*
358. *See* Beckmann, *supra* note 21, at 791; *see also* Blakeley, *supra* note 13.
359. Beckmann, *supra* note 21, at 791.
360. *See id.*
361. *See* Davidson, *supra* note 12.
362. *See id.*
363. *See* Miller & O'Rourke, *supra* note 13, at 847–53.

explaining to users how their information could be treated in case of bankruptcy[364] and (2) the Bankruptcy Code be amended to require enforcement of privacy policies or sale be allowed under terms similar to those in *Toysmart*.[365]

This solution balances the needs of customers and bankrupt companies. The conspicuous notice requirement clarifies consumer awareness about their rights to and control of their information. Moreover, it formalizes the FTC's solution in *Toysmart*, [366] creating a consistent rule for when failing Internet companies wish to sell customer information. The Toysmart solution also attempts to satisfy both customers and failed Internet companies.[367] Professors Miller and O'Rourke suggest that this solution will prevent websites from providing non-disclosure privacy policies[368] They also indicate that an ombudsman should be allowed to challenge a sale of a customer list and that some information should be considered unalienable and therefore absolutely prohibited from sale.[369] The professors admit that it is unclear whether Congress has the power to make certain information unalienable as it would generally fall under the realm of state power.[370]

While the Miller/O'Rourke solution is certainly the result of much greater consideration of all of the nuances of the problem, it does force creditors to bear the cost of the reduced value of customer lists. This is especially problematic in cases where a website does not have any privacy policy. The above solution forces companies to dictate a privacy policy and then restricts the sale of information that could have otherwise been sold without any legal challenge. Moreover, the restrictions that the Miller/O'Rourke solution suggests limits transferability, and as such, the value of such lists. Perhaps the creditors are those in the

364. *See id.* at 847–49.
365. *See id.* at 847–51.
366. *See supra* notes 234–37 and accompanying text.
367. *See supra* notes 234–37 and accompanying text.
368. *See* Miller & O'Rourke, *supra* note 13, at 850.
369. *See id.* at 852.
370. *See id.* (indicating that perhaps such a right could be imposed using the Commerce Clause of the Constitution).

best position to bear the risk,[371] but it is unlikely that they will support any solution that will devalue the estate.

Moreover, their solution does not address the problem of the sale of lists outside of bankruptcy, such as in a merger or acquisition.[372] Presumably, because the sale would not be objectionable to the professors because it would likely be to a company in a similar line of business. However, this is certainly not guaranteed[373] and for the sake of consistency, their solution should include the sale of all lists, not just those stemming from bankruptcy.

Despite the issues listed above, the Miller/O'Rourke solution certain addresses most of the concerns about the sale of customer lists and has the most merit.

CONCLUSION

There is clearly a conflict of interest between the goals of bankruptcy law and consumer privacy. However, what is more alarming is that customer data has been sold for many years without any protests from consumers. The sudden worries by Internet customers[374] are contrary to the lack of vocal interest of brick and mortar customers. It seems quite clear that customers of traditional brick and mortar businesses never really considered that their information was being saved and could ultimately be sold. It is time that consumer awareness about all data compilation is increased.

Certainly, any solution to the sale of customer data should be the same for Internet and traditional businesses. There should not be two different rules for two essentially identical failing businesses

---

371. *See generally* Rafael Efrat, *The Fresh-State Policy in Bankruptcy in Modern Day Israel*, 7 AM. BANKR. INST. L. REV. 555, 559 (1999) (discussing whether debtors or creditors are better risk-bearers).

372. *See supra* Part III.F.

373. *See supra* Part III.C (discussing how the Voter.com could have been sold to a partisan group that the subscribers did not agree with).

374. *See* Jones & Evans, *supra* note 51 (quoting Meg Smith, a fellow at Harvard University's Berkman Center for Internet and Society, as saying "[u]ntil we get the average person excited about this [sale of customer information], this isn't going to go anywhere [in terms of legislative change]").

simply because one is a brick and mortar store and the other exists only online. For example, a traditional pharmacy should not be able to sell its customer data when it fails while its Internet counterpart is prevented from doing so.

Aside from these concerns however, it is clear that a failing Internet business will have fewer legal concerns about selling a customer list if it is merged with or acquired by another company. Consumer privacy battles, for the moment, are confined to piecemeal bankruptcy or going out of business sales, where the successor in interest is bound to honor the policies of the company it has acquired.

FORDHAM JOURNAL OF CORPORATE & FINANCIAL LAW

Cite As 8 Fordham J. Corp. & Fin. L. [page] (2003)

The *Fordham Journal of Corporate & Financial Law* (ISSN 1532-303X) is published by student editors at Fordham University School of Law, 140 West 62nd Street, New York, New York 10023, U.S.A. Telephone: (212) 636-7008. Fax: (212) 636-6204. E-mail: jcfl@fordham.edu.

The *Journal* generally follows the conventions of *The Chicago Manual of Style* (14th ed. 1993). Citations generally conform to *The Bluebook: A Uniform System of Citation* (17th ed., Harvard Law Review Association). Citations to European Community materials generally conform to the *Citation Manual for European Community Materials*, available in Volume 21, Number 3 of the *Fordham International Law Journal*. The views expressed in the *Journal* are those of the authors and do not necessarily reflect the policies or opinions of the *Journal*, its editors and staff, Fordham Law School, or Fordham University.

INFORMATION FOR AUTHORS: The *Journal* welcomes unsolicited manuscripts from professional authors on issues of finance, securities and tax law, and related areas. The *Journal* does not publish articles by student authors unless they are studying for an advanced law degree at Fordham University. Authors should submit their manuscripts to the Senior Articles Editor or the Writing & Research Editor at the above-mentioned address, or by e-mail to jcfl@fordham.edu. We regret that mailed manuscripts cannot be returned except on receipt of return postage.

SUBSCRIPTION INFORMATION: The price for annual volumes is US$20.00 (US$24.00 foreign). Individual issues are US$10.00 each (US$14.00 foreign). The *Journal* renews subscriptions automatically unless notified to the contrary prior to expiration. Please address all subscription inquiries, orders for past volumes, and information regarding changes of address to the Business & Articles Editor.

For more information, please visit our Web site at:
http://law.fordham.edu/publications/jcfl.htm.